P3NK-3272-01Z0

IPアクセスルータ

Si-R シリーズ

Si-R 130B コマンドリファレンス

FUJITSU

はじめに

本書は、Si-R130B(以降、本装置と記載します) のコンソールから入力するコマンド について説明しています。

『本書の読み方』

本文中で使用しているマークについて説明します。

[機能] コマンド の機能概要を記載しています。

[入力形式]

入力形式を記載しています。以下の規約に従って記載しています。

< >	パラメタ名称を示しています。
[ ]	括弧内のオプションやパラメタを省略できることを示しています。
{ }	括弧内のオプションやパラメタのうち、いずれかを選択することを示しています。

[オプション]

各オプションの意味を記載しています。

[パラメタ]

各パラメタの意味を記載しています。

[説明] コマンド の解説を記載しています。

[注意] コマンド の注意事項を記載しています。

[例] コマンド の設定例、実行例または表示例を記載しています。

[未設定時]

コマンド の未設定時について説明し、設定したとみなされるコマンド を記載しています。

本文中で使用しているコマンド のパラメタに時間を指定する場合には、特別な指示がある場合を除き s(秒)、m(分)、h(時)、d(日) の単位をつけて設定します。

例： 1m = 1 分

なお、60s、60m、24h を指定した場合には、それぞれ、1m、1h、1d を指定したものとみなされます。

『使用上の注意事項』

本書の第 3 章から第 16 章までは、構成定義コマンドを説明しています。
構成定義コマンドを使用する場合には、以下の点にご注意ください。

- コマンドの設定および変更が終了したら、save コマンドを実行してから enable コマンドまたは reset コマンドを実行し、設定を有効にしてください。save コマンドを実行せず reset コマンドまたは電源再投入を行った場合にはコマンドの設定が元の状態に戻ります。また、save コマンドを実行せずに enable コマンドを実行した場合、一時的に設定は有効になりますが、reset コマンドまたは電源再投入を行った場合にコマンドの設定が元の状態に戻ります。ただし、password コマンドについては設定直後から有効となります。
- 構成定義コマンドを削除する場合は、delete を指定するか、未設定時の値を指定してください。delete の指定可否については、各コマンドの説明を参照してください。
- show コマンドにより構成定義を表示する場合、コマンド未設定時の値と同じ物は表示されません。コマンド未設定時の値を表示したい場合には、show コマンドに続けて、表示したいパラメタの直前のコマンドまで入力します。

[例]

LAN インタフェースの IP アドレスの表示

```
# show lan 0 ip address
192.168.1.1/24 3
```

平成 20 年 10 月

平成 20 年 10 月　初版

高度な安全性が要求される用途への使用について

本製品は，一般事務用，パーソナル用，家庭用，通常の産業等の一般的用途を想定して開発・設計・製造されているものであり，原子力施設における核反応制御，航空機自動飛行制御，航空交通管制，大量輸送システムにおける運行制御，生命維持のための医療用機器，兵器システムにおけるミサイル発射制御など，極めて高度な安全性が要求され，仮に当該安全性が確保されない場合，直接生命・身体に対する重大な危険性を伴う用途（以下「ハイセイフティ用途」という）に使用されるよう開発・設計・製造されたものではありません．

お客様は本製品を必要な安全性を確保する措置を施すことなくハイセイフティ用途に使用しないでください．また，お客様がハイセイフティ用途に本製品を使用したことにより発生する，お客様または第三者からのいかなる請求または損害賠償に対しても富士通株式会社およびその関連会社は一切責任を負いかねます．

お願い

- 本書を無断で他に転載しないようお願いします．
- 本書は予告なしに変更されることがあります．

目　次

第 1 章　ネットワーク設計概念

ここでは、本装置を利用してネットワークを設計する際に留意しなくてはならないネットワークの概念と、本装置のネットワーク定義の考え方について説明します。

1.1　ネットワークの概念とルーティング

1.1.1　ネットワークの考え方

ネットワークとは、通信手段を備えたコンピュータ同士がなんらかの伝送媒体を介して接続された集合体のことです。たとえば、HUB やスイッチなどの装置によって構築されたひとつの LAN はひとつのネットワークとなります。また一般加入線や専用回線などを利用して遠隔地を接続している WAN と呼ばれる部分についても、同様にひとつのネットワークとなります。

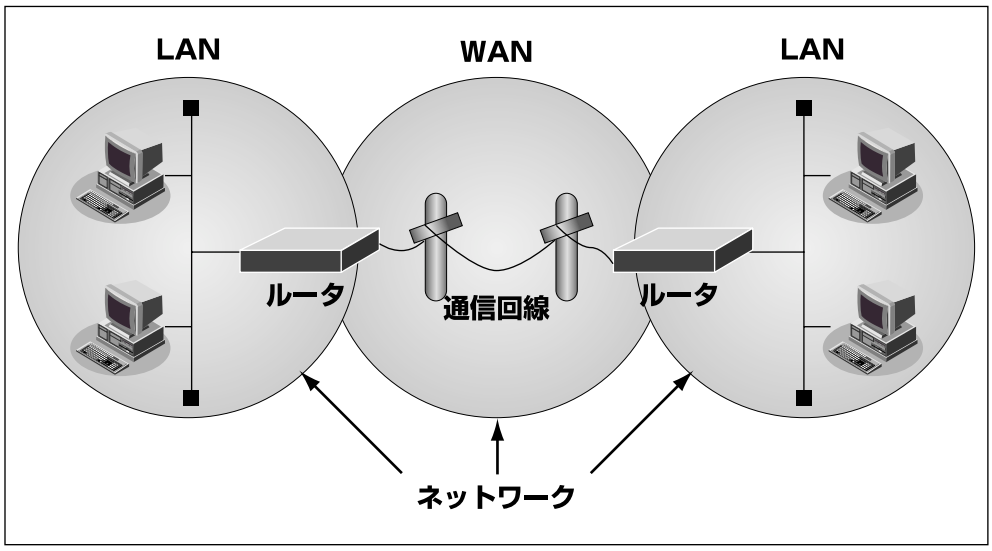


図 1.1　ネットワークの概念

また、広義の意味で、これらひとつひとつのネットワークが接続された全体に対してもネットワークと呼ばれます。

1.1.2 IP におけるネットワーク

IP ネットワークにおいては接続されるすべてのコンピュータ（ホスト）やルータなどのネットワーク機器にそれぞれユニークな IP アドレスを割り当てる必要があります。この IP アドレスは「ネットワーク部」と「ホスト部」から構成されます。

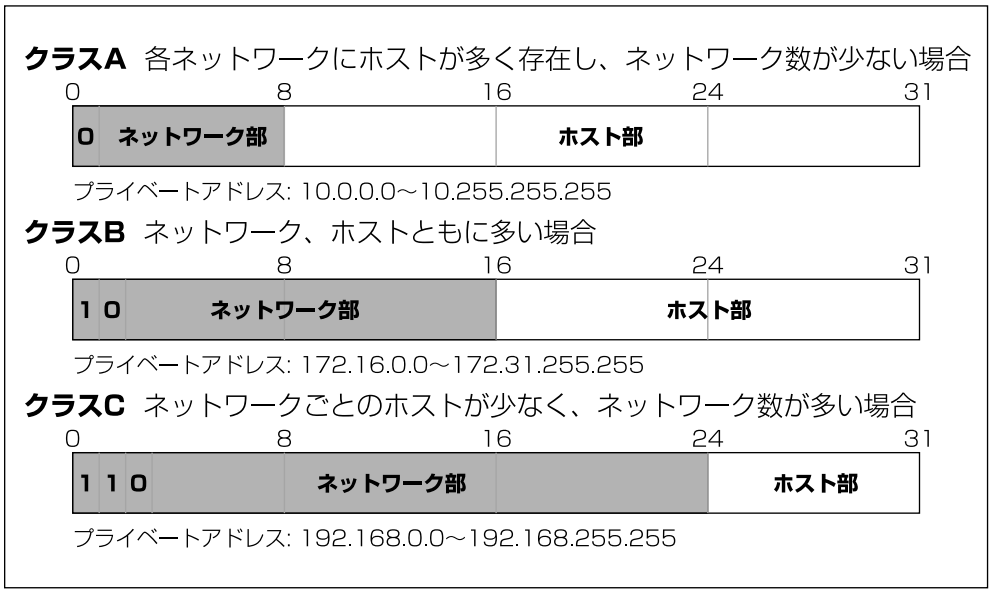


図 1.2 IP アドレスの構造

IP ネットワークにおけるひとつのネットワークとは、IP アドレスのネットワーク部が同一のアドレスを持つ機器の集まりとなります。つまり、同じデータリンクに接続される機器にはすべて同じネットワークアドレスを設定しなければなりません。さらに、ほかのデータリンクとネットワークアドレスが重ならないように割り当てる必要があります。

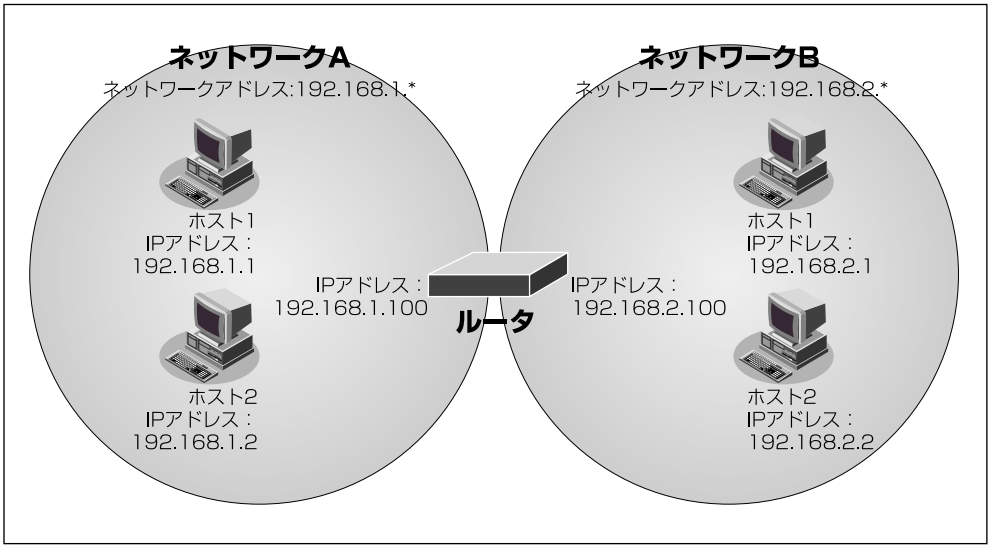


図 1.3 ネットワークとネットワークアドレス

以降、本書で単にネットワークと記述されている場合は IP の同一ネットワーク群のことを言います。また、広義のネットワークについては ”ネットワーク全体 ”と記述します。

1.1.3　ネットワークとルータ

本装置はネットワークとネットワークを相互に接続するルータと呼ばれる装置です。ルータは IP パケットと呼ばれる転送単位ごとに、パケットに付加されている IP アドレスのネットワーク部の情報に従って通信します。ほかのネットワーク宛のデータであればデータを転送することにより、ネットワーク間での通信を実現しています。この動作をルーティング（経路制御）と言い、このときにどのネットワークがどこにあるのかを知るために必要な情報がルーティング情報です。ルータはあらかじめ作成されたルーティング情報の集まりであるルーティングテーブル（経路制御表）によって動作します。ルーティングテーブルの作成方法には、管理者があらかじめ装置ごとに設定しておくスタティックルーティングと、接続されているルータ同士で情報を交換しあって自動的に作成するダイナミックルーティングの 2 種類の方法があります。

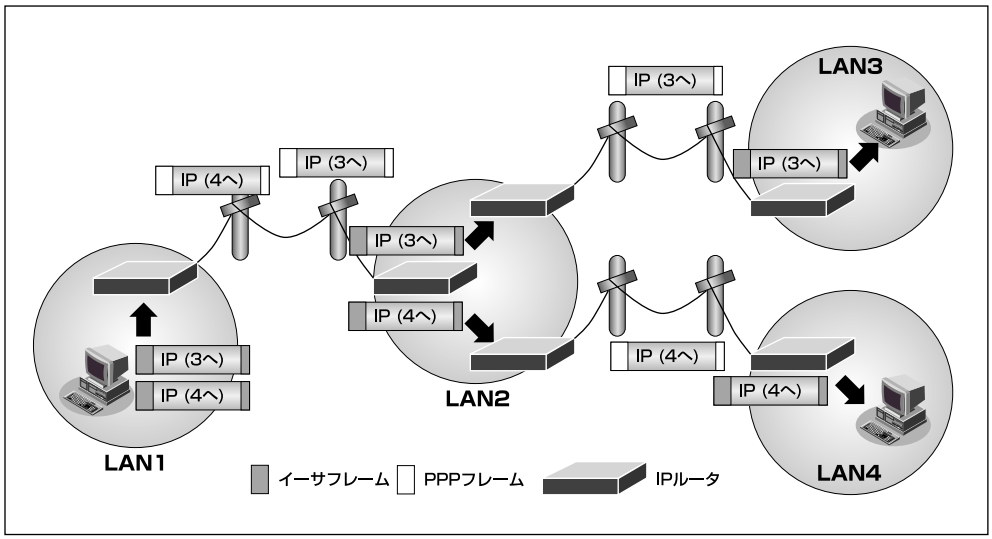


図 1.4　ルータの動作

なお、本装置では IP 以外のパケットを転送する機能であるブリッジについてもサポートしており、IP アドレスを持たない IP 以外のパケットについては Ethernet フレームの情報に従って適切な相手にデータを転送することもできます。

1.1.4 ネットワークインタフェースの概念

ルータがデータを送信または受信する場合には、論理的な出入り口が必要となります。この出入り口をネットワークインタフェースと呼び、すべてのデータの送受信はネットワークインタフェースを通じて行われます。

基本的にはネットワークインタフェースは物理回線と 1 対 1 に対応しますが、PPP 通信や tunnel 通信などのように物理回線と等価に見える論理的な通信路もあるため、ネットワークインタフェースはパケット転送処理のための論理的な出入り口と考える必要があります。

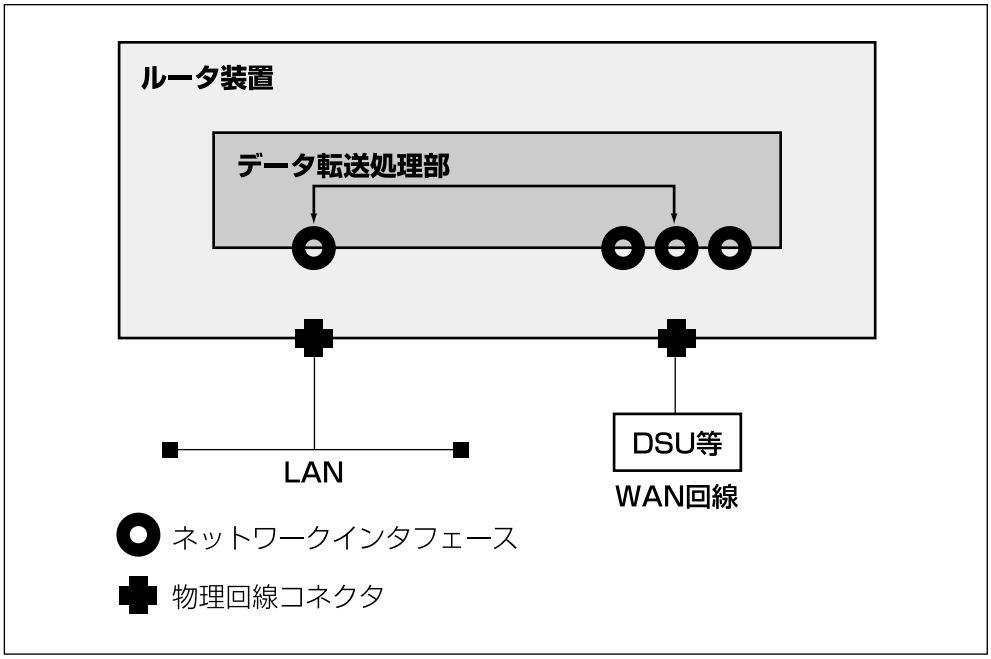


図 1.5　ネットワークインタフェース

1.1.5　ルーティングによる転送

ルーティングはネットワーク層プロトコルの情報によってデータの転送先を決定します。データ転送はパケットと呼ばれる通信単位ごとに転送先を選択し、転送先に対してデータを転送します。このとき、転送先を選択するための情報としてルーティングテーブル（経路制御表）を利用します。ルーティングテーブルとは「そのネットワークにデータを転送するためには、次にどの装置に対して転送したらよいか」を管理するテーブルです。ルーティングによる転送においては個々のパケットに含まれる宛先アドレスを元に経路情報を検索し、その経路に従って送出先を決定します。決定される情報は、出口となるネットワークインタフェースと、経由すべき次装置のアドレス (これは存在しない場合もあります) となります。

例：　192.168.2.1 宛のパケットを転送する場合

表 1.1　経路情報

宛先ネットワーク	次装置アドレス	出口インタフェース
192.168.1.0 / 24	—	lan0
192.168.2.0 / 24	192.168.1.2	lan0
:	:	:

この経路情報から、192.168.2.1 に到達するための出口となるネットワークインタフェースは lan0 であり、次装置は 192.168.1.2 であると判定されます。
この経路選択による出力先の選定は受信したデータに対してだけではなく、本装置が生成するデータについても同様に適用されます。つまり、経路情報が存在しないと装置からデータを送信することができません。このため、最低でも 1 つの経路情報を設定する必要あります。

1.1.6　ブリッジによる転送

もっとも簡単なブリッジによる転送の構造は、受信したデータをほかのすべてのネットワークインタフェースに対して送信します。しかし、これではトラフィックが膨大になるため、学習機能や制御プロトコルによって適切なネットワークインタフェースだけに転送することが一般的です。ルーティングと同じく、ここでもその出口ネットワークインタフェースの選定処理が行われます。

1.2 ルータ設定の概要

1.2.1 ネットワークと設定の関係

ルータに設定すべき情報としては、接続する回線に関する物理的な情報と、接続するネットワークに関する論理的な情報、そしてデータの振り分け条件であるルーティング情報が必ず必要となります。また、ほかに装置固有の情報や、付加的なサービスの設定を必要に応じて行います。
本装置ではこれらの情報の設定に関して大きく以下のように分類しています。

- wan 定義
  本装置に接続する回線に関する物理的な情報を定義する命令群であり、回線の種類や電話番号などの契約に関する情報を定義します。
- lan 定義
  本装置に接続する lan に関する論理的な情報を定義する命令群であり、lan のアドレスやネットワークの情報などを定義します。また、DHCP などの lan に固有のサービスに関しても lan 定義によって行います。
- remote 定義
  本装置が wan 回線を通じて通信を行う相手に関する論理的なネットワーク情報を定義する命令群であり、PPP に関する情報や相手ネットワークのアクセスポイントに関する情報などを定義します。
- answer 定義
  本装置が不特定の相手から接続される場合の情報を定義する命令群であり、必要に応じて定義します。
- その他の定義
  装置固有の情報や付加サービスの情報を必要に応じて定義する命令群であり、ネットワーク管理に関する情報や時刻情報などの定義があります。

各定義の分類と、実際のネットワークの対応を図 1.6 に示します。

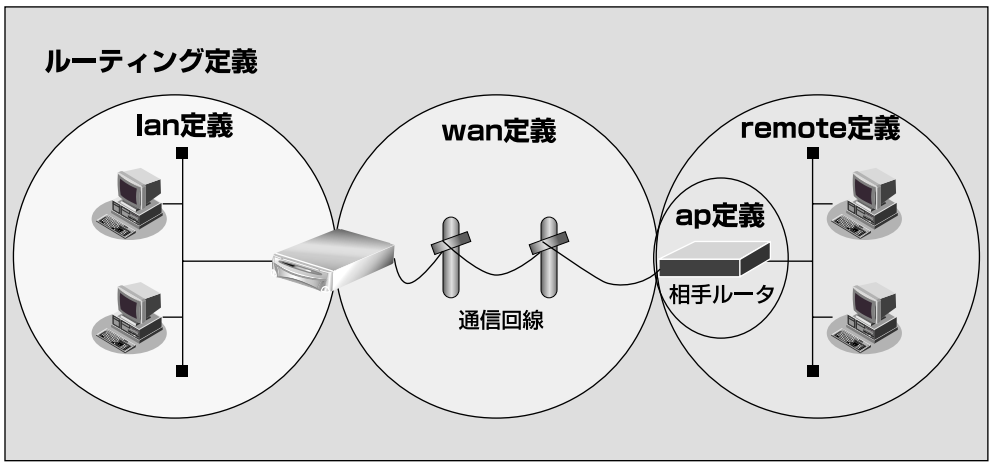


図 1.6　ネットワークと定義の対応

1.2.2　ネットワークインタフェースの定義

データ転送時の出口となるネットワークインタフェースには、その特性や接続されている回線によっていくつかの種別があります。

- lo

  ループバックインタフェース

  装置の内部プログラムで折返し通信を行う場合に利用されます。外部から利用することはありません。

- lan

  Etherent インタフェース

  Ethernet を利用して通信する場合に利用するネットワークインタフェースです。lan 定義によって設定されます。

- rmt

  設定済み相手用通信インタフェース

  ISDN / 専用線 / フレームリレーなどの回線を利用して通信を行う場合、または IPv6-over-IPv4 トンネルを利用して通信を行う場合に、定義された相手システムとの通信において利用されるネットワークインタフェースです。remote 定義によって設定されます。

これらのインタフェース種別にインタフェース番号を付与したものがネットワークインタフェース名となります。

例：　lo0, lan0, lan1, rmt0, rmt1, ...

lan および rmt のネットワークインタフェースはそれぞれ lan 定義、remote 定義によって設定されます。lan 定義、remote 定義の定義番号とネットワークインタフェースのインタフェース番号は 1 対 1 に対応します。lo は装置が自動設定しますので、設定項目はありません。

1.2.3　ルーティング情報の定義

ルーティング情報は最終的に出口となるネットワークインタフェースを決定するために必要な情報を定義するものです。本装置では出口インタフェースに対応する定義内でルーティング情報の設定を行います。たとえば、lan0 から出力するためのルーティング情報は lan0 内の定義に、rmt0 から出力するためのルーティング情報は remote0 内の定義に分けて設定します。

1.2.4 高度な転送先選定定義

本来の IP ルーティングにおける送信先選定のルールでは出力先インタフェースまでしか選定されません。このため、通常の IP ルーティングでは、1 つの経路によって決定される接続先は一つしか利用することができません。しかし、本装置では相手ネットワークの定義である remote 定義の配下に、実際の接続先設定となる ap 定義を複数定義することができます。これは、ルーティング情報によって決定された出力先の remote 定義の範囲で、送信データ内の宛先 IP アドレス以外の情報をルーティング情報の代わりに利用して、さらに送信先を分別するマルチルーティングという機能を利用して実現しています。たとえば、Internet と通信するためには default route というルーティング情報が必要ですが、ひとつの remote 定義において default route を設定した場合には、ほかの remote 定義には default route は設定できません。このため、remote 定義だけでは必要に応じて ISP を切り替えるということは通常の IP ルーティングの機構だけでは不可能です。本装置のマルチルーティングは、決定された remote 定義の範囲内でルーティング機構では参照されない情報を利用して、さらに細分化された送信先の選定を行います。
マルチルーティングは同一の remote 定義内で動作するため、remote 定義によるデータ送信先の分配と、ap 定義 (マルチルーティング) によるデータ送信先の分離は以下のように使い分けます。

- remote 定義による分離
  経路情報として分離できる接続先 (つまり、独立したネットワークとして識別できる接続先) は、それぞれ別の remote 定義として定義し、ルーティング機能を用いて分配を行います。
- ap 定義 (マルチルーティング) による分離
  経路情報では分離できない接続先 (つまり、独立したネットワークとして識別できない接続先) は、同一の remote 定義内にそれぞれ別の ap 定義として定義し、マルチルーティング機能を用いて分配を行います。

第 2 章　シェル機能

2.1　シェルを使う

本装置は、コマンドを入力して各種設定や表示などを行うことができます。
コマンドを入力するときに、入力を支援するのがシェルです。
シェルには、以下の機能があります。

- 文字入力機能
- 行編集機能
- 履歴機能
- コマンド名補完機能
- コマンド引数補完／説明表示／形式表示機能
- コマンド自動補完機能
- 環境変数機能

以下に、シェルの各機能について説明します。

文字入力機能

入力できる文字は、ASCII 文字、EUC 漢字またはシフト JIS 漢字です。漢字コードの種類は後述の環境変数で指定します。入力できる文字数は、プロンプト文字を含めて ASCII 文字で 1022 文字／行まで入力できます。漢字 1 文字は、ASCII 文字 2 文字分に相当します。

行編集機能

行編集機能とは、カーソルの移動、文字の挿入／削除などを行い、入力内容を編集する機能です。キー操作については、「キーバインド一覧」を参照してください。

履歴機能

入力した文字は、行単位で履歴として記憶されます。履歴機能とは、その履歴を表示したり、履歴を元に文字を編集したりしてコマンドを実行する機能です。キー操作については「キーバインド一覧」、履歴機能の詳細については「履歴機能詳細」を参照してください。

コマンド名補完機能

コマンド名補完機能とは、コマンド入力時にコマンド名を補完する機能です。コマンド入力時に、何も入力しない状態で［Tab］キーまたは［Ctrl+I］キーを押すと、コマンド名一覧が表示されます。
また、コマンド入力途中で［Tab］キーまたは［Ctrl+I］キーを押すと、入力途中の文字列で始まるコマンド名の補完候補を検索し、以下のように補完されるか、または候補一覧が表示されます。なお、入力途中で補完する場合は、カーソル位置直前の文字列が補完対象となります。カーソル位置以降の文字列は補完されません。

補完候補	動　作
見つからなかった場合	何も動作しません。
1つ見つかった場合	見つかったコマンド名を補完します。
複数見つかり、同じ文字が続く場合	同じ文字部分を補完します。
複数見つかり、異なる文字が続く場合	見つかったコマンド名を一覧表示します。

コマンド 引数補完／説明表示／形式表示機能

コマンド 引数補完／説明表示／形式表示機能とは、構成定義コマンド 入力時に引数を補完し、説明／形式を表示する機能です。
構成定義コマンド の引数入力時に［Tab］キーまたは［Ctrl+I］キーを 1 度押すと、コマンド 名補完と同様に引数が補完されます。
続けて［Tab］キーまたは［Ctrl+I］キーを押すと、引数の説明が表示されます。
さらに［Tab］キーまたは［Ctrl+I］キーを押すと、引数の形式が表示されます。
補完候補がない状態で［Tab］キーまたは［Ctrl+I］キーを押しても、補完および表示は行われません。
構成定義コマンド 以外の引数入力時に［Tab］キーまたは［Ctrl+I］キーを押すと、コマンド の入力形式が表示されます。ただし、一部のコマンド については何も表示されません。

補足　一部のコマンド では、カンマ（,）で区切って複数指定ができ、ハイフン（-）で区切って範囲指定ができます。ただし、引数補完時は、すべての引数で複数指定および範囲指定できるものとして処理され、カンマまたはハイフンを入力すると再びすべての引数候補が補完対象になります。

コマンド 自動補完機能

コマンド 自動補完機能とは、構成定義コマンド を続けて実行する際、直前に実行したコマンド の前部分が同じであることが多い場合に、直前に実行したコマンド の共通と思われる部分を自動的に入力する機能です。
コマンド 自動補完機能は、キー操作により有効／無効にすることができます。初期状態では無効です。有効にした場合でも、ログアウトすると自動的に無効になります。
詳しくは、「コマンド 自動補完機能詳細」を参照してください。

環境変数機能

環境変数機能とは、環境変数を利用してシェルの動作を指定する機能です。
環境変数は、env コマンド で設定、削除または表示することができます。
有効な環境変数名と値については、「有効な環境変数名と値」を参照してください。

2.2　シェル機能詳細

2.2.1　履歴機能詳細

履歴を展開する

入力行の最初に履歴展開指示子を入力して［Return］キーまたは［Enter］キーを押すと、履歴の内容が次の行に展開され、処理が実行されます。
履歴展開指示子は、入力行の最初に 1 度だけ指定できます。それ以降に指定した場合は、入力文字とみなされます。
また、履歴展開指示子の後ろに入力した文字は、展開された履歴の後ろに入力され、実行されます。
以下に、履歴展開指示子とその動作について示します。

履歴展開指示子	動　作
!!	直前の履歴を展開します。
!履歴番号	指定した番号の履歴を展開します。
!-履歴数	現在の履歴番号から指定した履歴数前の履歴を展開します。
!文字列	指定した文字列で始まる最新の履歴を展開します。

以下に、実行例を示します。

●コマンド

```
# netstat
（netstat の実行結果が表示される）

# !! -a
netstat -a          ：履歴展開結果が表示される
（netstat  -a の実行結果が表示される）

#
```

直前履歴の文字列を置換する

直前履歴の文字列を置換して処理を実行するか、または文字列置換後の直前履歴を表示することができます。なお、表示する場合、処理の実行は行われません。

文字列を置換し実行する場合

以下のように直前履歴置換指示子（^）に続けて、検索する文字列と置換する文字列を入力します。

```
^検索文字列^置換文字列^
```

文字列置換後の直前履歴が表示されて、処理が実行されます。
以下に、実行例を示します。

●コマンド

```
# show lan 0 ip address
（lan0 のアドレスが表示される）

#  ^address^alias^
show lan 0 ip alias                    ：文字列置換後の直前履歴が表示される

（lan0 のセカンダリ IP アドレスが表示される）

#
```

また、置換指示に続けて文字列を入力すると、入力した文字列が最後に追加されて実行されます。

```
^検索文字列^置換文字列^追加文字列（置換および追加して実行）
```

文字列を置換し表示する場合

以下のように、置換指示に続けて表示指示子（:p）を入力します。

```
^検索文字列^置換文字列^:p
```

文字列置換後の直前履歴が表示されます。処理は実行されません。
表示された内容は履歴として記憶されます。
また、表示指示に続けて文字列を入力すると、入力した文字列が最後に追加されて表示されます。

```
^検索文字列^置換文字列^:p 追加文字列（置換および追加した状態を表示）
```

直前履歴の文字列を削除する

指定した文字列を直前履歴から削除して処理を実行するか、または文字列削除後の直前履歴を表示することができます。なお、表示する場合、処理の実行は行われません。

文字列を削除し実行する場合

以下のように、直前履歴置換指示子（^）に続けて、削除する文字列を指定します。

```
^削除文字列^^
```

文字列削除後の直前履歴が表示されて、処理が実行されます。
また、削除指示に続けて文字列を入力すると、入力した文字列が最後に追加されて実行されます。

```
^検索文字列^^追加文字列（削除および追加して実行）
```

文字列を削除し表示する場合

以下のように、削除指示に続けて表示指示子（:p）を入力します。

```
^削除文字列^^:p
```

文字列削除後の直前履歴が表示されます。処理は実行されません。
表示された内容は履歴として記憶されます。
また、表示指示に続けて文字列を入力すると、入力した文字列が最後に追加されて表示されます。

```
^検索文字列^^:p 追加文字列（削除および追加した状態を表示）
```

履歴の文字列を置換する

履歴の文字列を置換して処理を実行するか、または処理を実行せずに文字列置換後の履歴を表示することができます。

補足　履歴の文字列置換時に指定する区切り文字には、任意の文字を指定できます。ただし、行単位で同じ区切り文字を指定してください。

以下に例を示します。

- :s@検索文字列@置換文字列@　（一置換）
- :gs%検索文字列%置換文字列%　（全置換）
- :ps^検索文字列^置換文字列^　（一置換履歴表示）
- :pgs_検索文字列_置換文字列_　（全置換履歴表示）

文字列を置換し実行する場合

一置換履歴指示子（:s）、全置換履歴指示子（:g）に続けて、検索する文字列と置換する文字列を入力します。なお、:g は、:s と共に指定してください。
以下に、組み合わせを示します。

```
:s/検索文字列/置換文字列/          一置換
:gs/検索文字列/置換文字列/         全置換
```

文字列置換後の履歴が表示されて、処理が実行されます。

文字列を置換し表示する場合

一置換または全置換指示と共に表示指示子（:p）を入力します。
以下に、組み合わせを示します。

```
:ps/検索文字列/置換文字列/         一置換履歴表示
:pgs/検索文字列/置換文字列/        全置換履歴表示
```

文字列置換後の履歴が表示されます。処理は実行されません。
以下に、実行例を示します。

●コマンド

```
#  remote 0 ip address local 192.168.0.1
# !!:pgs/0/1/
remote 1 ip address local 192.168.1.1       : 実行せずに表示だけ
# !!
remote 1 ip address local 192.168.1.1       : 実行される
```

以下のように、連続して指定することもできます。

```
:s/検索文字列1/置換文字列1/:gs/検索文字列2/置換文字列2/:p      （一置換と全置換の履歴を表示）
```

また、置換指示に続けて文字列を入力すると、入力した文字列が最後に追加されて実行されます。

```
:s/検索文字列/置換文字列/追加文字列      （一置換および追加して実行）
```

履歴の文字列を削除する

指定した文字列を履歴から削除して処理を実行するか、または処理を実行せずに削除後の履歴を表示することができます。

補足　履歴の文字列削除時に指定する区切り文字には、任意の文字を指定できます。ただし、行単位で同じ区切り文字を指定してください。

以下に例を示します。

- :s@削除文字列@@　（一削除）
- :gs%削除文字列%%　（全削除）
- :ps^削除文字列^^　（一削除履歴表示）
- :pgs_削除文字列__　（全削除履歴表示）

文字列を削除し実行する場合

一置換履歴指示子（:s）、全置換履歴指示子（:g）に続けて、削除する文字列を入力します。なお、:g は、:s と共に指定してください。
以下に、組み合わせを示します。

```
:s/削除文字列//          一削除
:gs/削除文字列//         全削除
```

文字列削除後の履歴が表示されて、処理が実行されます。

文字列を削除し表示する場合

削除指示と共に表示指示子（:p）を入力します。
以下に、組み合わせを示します。

```
:ps/削除文字列//          一削除履歴表示
:pgs/削除文字列//         全削除履歴表示
```

文字列削除後の履歴が表示されます。処理は実行されません。
また、置換指示に続けて文字列を入力すると、入力した文字列が最後に追加されて表示されます。

```
:gs/削除文字列//追加文字列                    （全削除および追加して実行）
:s/削除文字列//:gs/検索文字列/置換文字列/:p 追加文字列
                                              （一削除、全置換および追加して表示）
```

ヒント　履歴機能使用時の最後の区切り文字は省略できます。ただし、省略した場合は、表示指示子（:p）、連続指定、または追加文字列を指定することができません。

- ^検索文字列^置換文字列
- ^削除文字列
- :s/検索文字列/置換文字列
- :gs/削除文字列
- :s/削除文字列/ /:pgs/削除文字列

2.2.2　コマンド 自動補完機能詳細

Ctrl+O を入力すると、以下のメッセージが表示されます。コマンド 自動補完機能が有効になります。入力途中の内容は破棄されません。

```
Auto-completion is enabled. To disable, type Ctrl+G.
```

Ctrl+G を入力すると、以下のメッセージが表示されます。コマンド 自動補完機能が無効になります。入力途中の内容は破棄されます。

```
Auto-completion is disabled.
```

ログアウトすると、コマンド 自動補完機能は無効になります。メッセージは表示されません。
コマンド 自動補完機能が有効のときに構成定義コマンド を実行すると、コマンド および引数の共通部分が自動的に入力されます。

例）

```
# lan 0 ip address 192.168.1.1/24 3          構成定義コマンド を実行します
# lan 0 ip                                   自動的に入力されます
# lan 0 ip dhcp service server               続きを入力します
# lan 0 ip dhcp                              自動的に入力されます
# lan 0 ip dhcp info address 192.168.1.100/24 続きを入力します
# lan 0 ip dhcp info                         自動的に入力されます
```

自動的に入力された内容が不要な場合は、Ctrl+U または Ctrl+C を入力してください。Ctrl+W を入力するとカーソル直前の引数（1 単語）を削除することができます。
コマンド によっては、自動入力内容が不足したり、余計だったりすることがありますので、注意してください。

2.2.3 有効な環境変数名と値

以下に、シェルを使用するときに有効な環境変数名と値を示します。

環境変数名	値
PROMPT	プロンプト文字列 空白を含める場合は、「"」（ダブルクォート）で囲みます。 PS1を指定しない場合、"\u\p"が指定されたものとみなされます。 以下の特殊文字を含めると、展開して置き換えます。 \! : 履歴番号 \p : 標準プロンプト（「>」または「#」） \u : 環境変数USER（ログオン前は無効） \U : 環境変数USER（ログオン前も有効） \\ : バックスラッシュ \その他 : その他
COLUMNS	画面桁数 端末エミュレータの画面桁数を指定します。 無効な値（0以下、数字以外）を指定すると、変更されません。 実際の桁数と異なる値を指定すると、表示やカーソル位置が乱れます。 telnetを使用する場合、ログオン時と画面サイズ変更時にシェル内部の桁数が自動更新され、環境変数値は無視されます。 ただし、本環境変数を設定すると、次にログオンまたは画面サイズを変更するまで、本環境変数値が用いられます。
LINES	画面行数 端末エミュレータの画面行数を指定します。 無効な値（0以下、数字以外）を指定すると、変更されません。 13以下を指定すると、表示やカーソル位置が乱れます。 telnetを使用する場合、ログオン時と画面サイズ変更時にシェル内部の桁数が自動更新され、環境変数値は無視されます。 ただし、本環境変数を設定すると、次にログオンまたは画面サイズを変更するまで、本環境変数値が用いられます。
KANJI	漢字コード コマンド引数説明表示時に使用する漢字コードを指定します。 SJIS : ShiftJIS漢字コード それ以外: EUC漢字コード 削除 : EUC漢字コード
USER	利用者名 環境変数PROMPTの／uや／Uで使用する文字列を指定します。
NOBELL	ベル動作 以下のような場合、シェルはベルを鳴らします。 制限文字数（1022文字）を超えて入力しようとした場合 制限文字数（1022文字）を超える貼り付けを行った場合 補完候補がない場合 本環境変数の指定値によって、鳴らないようにできます。 yes : 鳴らない on : 鳴らない それ以外: 鳴る 削除 : 鳴る
HISTSIZE	履歴行数 コマンド履歴行数を指定します。 無効な値（数字以外）を指定すると、変更されません。

2.2.4　キーバインド 一覧

以下に、シェルを使用するときのキーバインド を示します。

組合せキー（注）	単一キー	動　作
Ctrl+A		カーソルを先頭に移動
Ctrl+B	←（注）	カーソルを一文字左に移動
Ctrl+C		入力中断
Ctrl+D		入力文字があるときは一文字削除 入力文字がないときはログオフ
Ctrl+E		カーソルを末端に移動
Ctrl+F	→（注）	カーソルを一文字右に移動
Ctrl+G		自動補完無効
Ctrl+H	BS	カーソルを一文字左に移動して一文字削除
Ctrl+I	Tab	補完／補完候補一覧表示／引数説明表示／引数形式表示
Ctrl+J	Return	入力完了
Ctrl+K		カーソル位置から末端までを切り取り
Ctrl+L		画面更新
Ctrl+M		入力完了
Ctrl+N	↓（注）	次履歴
Ctrl+O		自動補完有効
Ctrl+P	↑（注）	前履歴
Ctrl+R		入力再表示
Ctrl+T		一文字交換
Ctrl+U		カーソル位置から先頭までを切り取り
Ctrl+W		カーソル位置から一単語左までを切り取り
Ctrl+X		カーソル位置から先頭までを切り取り
Ctrl+Y		貼り付け
ESC Ctrl+I	ESC TAB	引数説明表示
ESC Ctrl+K		カーソル位置から一単語右までを切り取り
ESC b		カーソルを一単語左に移動
ESC f		カーソルを一単語右に移動
ESC <		最古履歴
ESC >		最新履歴

注）

- Ctrl+ α は、［Ctrl］キー（または［control］キー）を押しながら［ α ］キーを押すことを示しています。
- ESC α は、［ESC］キーを押してから、［ α ］キーを押すことを示しています。
- ハイパーターミナルでは矢印キー（↑、↓、←、→）が正しく動作しません。組み合わせキーを使用してください。

- ターミナルソフトウェアや telnet コマンドで使用する場合、1 部の Ctrl+ α のキーが入力できない場合があります。その場合、ターミナルソフトウェアや telnet コマンドのマニュアルを参照し、Ctrl+ α が入力できるように設定を変更してください。

第 3 章　回線情報の設定

3.1　回線共通情報

3.1.1　wan line

[機能]

回線インタフェースおよび通信速度の設定

[入力形式]

wan [<number>] line isdn (ISDN)
wan [<number>] line hsd <speed> (専用線)
wan [<number>] line fr <speed> (フレームリレー)

[パラメタ]

<number>

- wan 定義番号
  wan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<speed>

- 回線速度
  専用線またはフレームリレー利用時の回線速度を以下の範囲で指定します。
  64k, 128k

[説明]

wan 定義で利用する回線の、回線種別を設定します。

[未設定時]

回線種別として ISDN を設定したものとみなされます。回線種別は必ず設定してください。

```
wan <number> line isdn
```

3.2 ISDN 回線情報

3.2.1 wan isdn global

[機能]

グローバル着信の設定

[入力形式]

wan [<number>] isdn global <mode>

[パラメタ]

<number>

- wan 定義番号
  wan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<mode>

グローバル着信を受け付けるかどうかを指定します。

- accept
  グローバル着信を受け付けます。
- reject
  グローバル着信を受け付けません。

[説明]

グローバル着信を受け付けるかどうかを設定します。
通常は<mode>に accept を指定してください。ただし、ダイヤルイン番号または i・ナンバー宛の着信だけを受け付ける場合は reject を指定し、“3.2.2 wan isdn number” で着信を受け付ける着信番号を指定してください。

[未設定時]

グローバル着信を受け付けるものとみなされます。

```
wan <number> isdn global accept
```

3.2.2　wan isdn number

[機能]

自局電話番号の設定

[入力形式]

wan [<number>] isdn number <count> <tel_number> [<subaddress>]

[パラメタ]

<number>

- wan 定義番号
  wan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<count>

着信番号チェックを行う電話番号は、2 組まで設定できます。2 組のうちのどちらを設定するか、番号を指定します。

- 0
  着信番号チェックの電話番号 1 を設定します。
- 1
  着信番号チェックの電話番号 2 を設定します。

<tel_number>

着信番号チェックを行う電話番号を指定します。

- 電話番号
  着信時にチェックする電話番号を、0～9 の数字と、*、#、-、(、)、\の文字で構成される 32 桁以内の ASCII 文字列で指定します。
- any
  着信番号チェックを行わない場合に指定します。
  なお、<subaddress>を指定する場合は、<subaddress>だけを着信番号チェックの対象とします。
- in1
  i・ナンバーサービス契約時に、i・ナンバー情報 1(契約者回線番号) の着信を受け付ける場合に指定します。
- in2
  i・ナンバーサービス契約時に、i・ナンバー情報 2(追加の番号) の着信を受け付ける場合に指定します。
- in3
  i・ナンバーサービス契約時に、i・ナンバー情報 3(追加の番号) の着信を受け付ける場合に指定します。

<subaddress>

- サブアドレス
  着信時にチェックするサブアドレスを、0x22(ダブルクォーテーション) を除くコードで構成される 19 桁以内の ASCII 文字列で指定します。省略した場合は、サブアドレスをチェックしません。

[説明]

着信番号チェックについて設定します。
ダイヤルイン番号、i・ナンバー、サブアドレスを利用して着信機器を識別するかどうかを、<tel_number>と<subaddress>の組み合わせで指定します。着信番号チェックの電話番号は、2 組まで設定できます。
着信時に網から通知される電話番号とサブアドレスが着信番号チェックの電話番号と一致しない場合は、着信を受け付けません。
<tel_number>に any を指定し、かつ<subaddress>を指定した場合は、<subaddress>だけが着信番号チェックの対象となります。また、<tel_number>に any を指定し、<subaddress>が未指定の場合は、着信番号チェックをしません。
i・ナンバーサービス契約時は、<tel_number>に in1、in2、または in3 のいずれかを指定してください。

[未設定時]

着信番号チェックを行わないとみなされます。

```
wan <number> isdn number 0 any
```

3.2.3　wan isdn numbersend

[機能]

発信者番号通知の設定

[入力形式]

wan [<number>] isdn numbersend <mode> [<tel_number> [<subaddress>]]

[パラメタ]

<number>

- wan 定義番号
  wan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<mode>

発信者番号の通知形態を指定します。

- specified
  <tel_number>および<subaddress>で指定する電話番号を、発信者番号として通知します。
- default
  網契約に従います。回線の加入契約で選択した内容の設定になります。
- off
  接続先に発信者の電話番号を通知しません。

以下のパラメタは、<mode>に specified を設定した場合にだけ有効です。

<tel_number>

<mode>に specified を設定した場合、必ず以下のいずれかを指定してください。

- 通知電話番号
  発信者番号として通知する電話番号を、0〜9 の数字と、*、#、-、(、)、\の文字で構成される 32 桁以内の ASCII 文字列で指定します。
- in1
  発信者番号として、i・ナンバー情報 1 を通知します。
- in2
  発信者番号として、i・ナンバー情報 2 を通知します。
- in3
  発信者番号として、i・ナンバー情報 3 を通知します。

<subaddress>

- サブアドレス
  発信者番号の一部として通知するサブアドレスを、0x22(ダブルクォーテーション) を除くコードで構成される 19 桁以内の ASCII 文字列で指定します。省略した場合は、サブアドレスを通知しません。

[説明]

発信者番号を通知するかどうかを設定します。また。通知する場合の、通知番号を設定します。

[未設定時]

網契約に従うとみなされます。

```
wan <number> isdn numbersend default
```

3.2.4　wan isdn limit charge

[機能]

上限課金額による (発呼抑止) 条件の設定

[入力形式]

wan [<number>] isdn limit charge <charge> [<diallock>]

[パラメタ]

<number>

- wan 定義番号
  wan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<charge>

- 上限課金額
  自動発信を制限する上限課金額を、0〜999999 の 10 進数値 (単位:円) で指定します。0 を指定した場合は、課金額による自動発信制限を行いません。

<diallock>

自動発信を制限するかどうかを指定します。

- yes
  上限課金額に達した場合に、以降の自動発信を制限します。
  ただし、回線の手動接続は、制限の対象外となります。
- no
  上限課金額に達した場合に、以降の自動発信を制限しません。

省略した場合は、yes を指定したものとみなされます。

[説明]

データ通信において、通信課金の累計が上限課金額に達した場合に、自動発信を制限するかどうかを設定します。
<diallock>の指定内容にかかわらず、<charge>で指定した上限課金額を超えて自動発信しようとした場合は、syslog が採取されます。

[未設定時]

課金額による自動発信制限を行わないとみなされます。

```
wan <number> isdn limit charge 0 yes
```

3.2.5 wan isdn limit time

[機能]

上限通信時間による (発呼抑止) 条件の設定

[入力形式]

wan [<number>] isdn limit time <time> [<diallock>]

[パラメタ]

<number>

- wan 定義番号
  wan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<time>

- 上限接続時間
  自動発信を制限する接続時間の上限時間を、0 秒～999 時間の 10 進数値で指定します。単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。
  0 を指定した場合は、接続時間による自動発信制限を行いません。

<diallock>

自動発信を制限するかどうかを指定します。

- yes
  接続時間の上限に達した場合に、以降の自動発信を制限します。
  ただし、回線の手動接続は、制限の対象外となります。
- no
  接続時間の上限に達した場合に、自動発信を制限しません。

省略した場合は、yes を指定したものとみなされます。

[説明]

データ通信において、通信時間の累計が接続時間の上限に達した場合に、自動発信を制限するかどうかを設定します。
<diallock>の指定内容にかかわらず、<time>で指定した上限接続時間を超えて自動発信しようとした場合は、syslog が採取されます。

[未設定時]

接続時間による自動発信制限を行わないとみなされます。

```
wan <number> isdn limit time 0d yes
```

3.2.6　wan isdn accept

[機能]

装置単位の着信可否の設定

[入力形式]

wan [<number>] isdn accept <mode>

[パラメタ]

<number>

- wan 定義番号
  wan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<mode>

データ着信時の動作について指定します。

- enable
  “5.2.24 remote ap called accept” の設定に従います。
- disable
  着信を禁止します。着信をすべて拒否し、発信専用の装置となります。

[説明]

外部から本装置に着信したときの動作について設定します。

[未設定時]

“5.2.24 remote ap called accept” の設定に従うものとみなされます。

```
wan <number> isdn accept enable
```

3.2.7 wan isdn autodial

[機能]

装置単位の自動発信可否の設定

[入力形式]

wan [<number>] isdn autodial <mode>

[パラメタ]

<number>

- wan 定義番号
  wan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<mode>

自動的にダイヤルするかどうかについて指定します。

- enable
  “5.1.3 remote autodial” の設定に従います。
- disable
  本装置からの自動ダイヤルを禁止します。どのような通信データが発生した場合も、自動的にはダイヤルしません。

[説明]

通信データが発生したときに、自動的にダイヤルするかどうかを設定します。

[未設定時]

“5.1.3 remote autodial” の設定に従います。

```
wan <number> isdn autodial enable
```

3.2.8　wan isdn keeptime

[機能]

テレホーダイ機能デフォルト時間の設定

[入力形式]

wan [<number>] isdn keeptime <time>

[パラメタ]

<number>

- wan 定義番号
  wan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<time>

- 初期時間
  回線接続保持の初期時間を、0 秒～86400 秒 (1 日) の範囲で指定します。単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。

[説明]

テレホーダイ機能 (回線接続保持機能) が時間指定なしで起動された場合のデフォルト時間を設定します。0 が設定された場合にはデフォルト時間はないものとして扱われ、timerctl コマンドによりテレホーダイ機能 (回線接続保持時間) を起動するときに接続保持時間の指定が必要となります。

[注意]

この定義は、wan line コマンドで isdn が設定されているもっとも<number>の小さい wan 定義に設定されているものだけが有効です。

[未設定時]

デフォルト時間はありません。

```
wan <number> isdn keeptime 0d
```

3.3 フレームリレー回線情報

3.3.1 wan fr lmi

[機能]

フレームリレーにおける PVC 状態確認手順の設定

[入力形式]

wan [<number>] fr lmi <type>

[パラメタ]

<number>

- wan 定義番号
  wan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<type>

PVC 状態確認の手順を指定します。

- q933a
  ITU-T Q.933 Annex A に準拠します。
- off
  PVC 状態確認を行いません。

[説明]

フレームリレーでの PVC 状態確認手順を、網契約に合わせて設定します。

[注意]

- この機能を使用する場合は、通信事業者との契約が必要です。
- PVC 状態確認の双方向手順はサポートしていません。

[未設定時]

ITU-T Q.933 Annex A に準拠するとみなされます。

```
wan <number> fr lmi q933a
```

3.3.2　wan fr fecn

[機能]

FECN による輻輳制御の設定

[入力形式]

wan [<number>] fr fecn <mode>

[パラメタ]

<number>

- wan 定義番号
  wan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<mode>

FECN によって輻輳制御を行うかどうかを指定します。

- on
  輻輳制御を行います。
- off
  輻輳制御を行いません。

[説明]

FECN による輻輳制御について設定します。

[未設定時]

FECN によって輻輳制御を行うとみなされます。

```
wan <number> fr fecn on
```

3.3.3 wan fr becn

[機能]

BECN による輻輳制御の設定

[入力形式]

wan [<number>] fr becn <mode>

[パラメタ]

<number>

- wan 定義番号
  wan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<mode>

BECN によって輻輳制御を行うかどうかを指定します。

- on
  輻輳制御を行います。
- off
  輻輳制御を行いません。

[説明]

BECN による輻輳制御について設定します。

[未設定時]

BECN によって輻輳制御を行うとみなされます。

```
wan <number> fr becn on
```

3.3.4　wan fr cllm

[機能]

CLLM による輻輳制御の設定

[入力形式]

wan [<number>] fr cllm <mode>

[パラメタ]

<number>

- wan 定義番号
  wan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<mode>

CLLM によって輻輳制御を行うかどうかを指定します。

- on
  輻輳制御を行います。
- off
  輻輳制御を行いません。

[説明]

CLLM による輻輳制御について設定します。

[未設定時]

CLLM によって輻輳制御を行うとみなされます。

```
wan <number> fr cllm on
```

第 4 章　LAN 情報の設定

4.1　IP 関連情報

4.1.1　lan ip address

[機能]

IP アドレスの設定

[入力形式]

lan [<number>] ip address <address> / <mask> <broadcast>

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<address>/<mask>

- IP アドレス / マスクビット数 (またはマスク値)
  LAN インタフェースに割り当てる IP アドレスとマスクビット数の組み合わせを指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。
  以下に、有効な記述形式を示します。
  - IP アドレス / マスクビット数 (例: 192.168.1.1 / 24)
  - IP アドレス / マスク値 (例: 192.168.1.1 / 255.255.255.0)

なお、IP アドレスに 0.0.0.0 を指定すると、通信できなくなります。

<broadcast>

ブロードキャストアドレスを指定します。

- 0
  0.0.0.0 の場合に指定します。
- 1
  255.255.255.255 の場合に指定します。
- 2
  <address> / <mask>から求められる、ネットワークアドレス + オール 0 の場合に指定します。
- 3
  <address> / <mask>から求められる、ネットワークアドレス + オール 1 の場合に指定します。

[説明]

本装置上の LAN インタフェースに、IP アドレス、マスクビット数 (またはマスク値)、およびブロードキャストアドレスを設定します。
LAN インタフェースに割り当てる IP アドレス、ネットマスクを設定します。IP アドレスを設定していないと通信できません。

[未設定時]

IP アドレスがないものとみなされます。

```
lan <number> ip address 0.0.0.0 0
```

4.1.2 lan ip alias

[機能]

セカンダリ IP アドレスの設定

[入力形式]

lan [<number>] ip alias <address>/<mask> <broadcast>

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<address>/<mask>

- セカンダリ IP アドレス/マスクビット数 (またはマスク値)
  LAN インタフェースに割り当てるセカンダリ IP アドレスとマスクビット数の組み合わせを指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。
  以下に、有効な記述形式を示します。
  - セカンダリ IP アドレス/マスクビット数 (例: 192.168.1.1/24)
  - セカンダリ IP アドレス/マスク値 (例: 192.168.1.1/255.255.255.0)

<broadcast>

ブロードキャストアドレスを指定します。

- 0
  0.0.0.0 の場合に指定します。
- 1
  255.255.255.255 の場合に指定します。
- 2
  <address>/<mask>から求められる、ネットワークアドレス + オール 0 の場合に指定します。
- 3
  <address>/<mask>から求められる、ネットワークアドレス + オール 1 の場合に指定します。

[説明]

本装置上の LAN インタフェースに、セカンダリ IP アドレス、マスクビット数 (またはマスク値)、およびブロードキャストアドレスを設定します。

[注意]

セカンダリ IP アドレスが属するネットワークには、以下の機能を適用できません。

- RIP の送受信機能
- DHCP 機能

[未設定時]

セカンダリ IP アドレスがないものとみなされます。

```
lan <number> ip alias 0.0.0.0 0
```

4.1.3 lan ip dhcp service

[機能]

DHCP 機能の設定

[入力形式]

lan [<number>] ip dhcp service <mode> [<address1> [<address2>]]

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<mode>

DHCP 機能のモードを指定します。

- server
  LAN インタフェースに対して DHCP サーバサービスを行います。
- relay
  LAN インタフェースに対して DHCP リレーエージェントサービスを行います。
- off
  LAN インタフェースに対して DHCP 機能を提供しません。

<address1>,<address2>

- DHCP サーバアドレス
  <mode>に relay を指定した場合に有効なパラメタです。DHCP サービス要求を転送する、中継先 DHCP サーバの IP アドレスを 2 つまで指定することができます。

[説明]

LAN インタフェースに対して、DHCP 機能情報を設定します。

[未設定時]

DHCP サーバ機能を使用しないものとみなされます。

```
lan <number> ip dhcp service off
```

4.1.4　lan ip dhcp info

[機能]

DHCP 配布情報の設定

[入力形式]

lan [<number>] ip dhcp info dns <dns1> [<dns2>]
lan [<number>] ip dhcp info address <address>/<mask> [<num>]
lan [<number>] ip dhcp info time <time>
lan [<number>] ip dhcp info gateway <gateway>
lan [<number>] ip dhcp info domain [<domain>]

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<dns1>

- DNS サーバ IP アドレス
  DHCP クライアントに配布する、DNS サーバの IP アドレスを指定します。
  0.0.0.0 を指定した場合は、設定が削除されます。

<dns2>

- セカンダリ DNS サーバ IP アドレス
  DHCP クライアントに配布する、セカンダリ DNS サーバの IP アドレスを指定します。
  0.0.0.0 を指定した場合は、設定が削除されます。

<address>/<mask>

- 割り当て開始 IP アドレス/マスクビット数 (またはマスク値)
  DHCP クライアントにリースする先頭アドレス (IP アドレスとマスクビット数の組み合わせ) を指定します。
  マスク値は、最上位ビットから 1 で連続した値にしてください。
  以下に、有効な記述形式を示します。

  ー　IP アドレス/マスクビット数 (例: 192.168.1.2/24 注)
  ー　IP アドレス/マスク値 (例: 192.168.1.2/255.255.255.0 注)

  <num>が 16、<address>が 192.168.1.2 の場合に、192.168.1.2～192.168.1.17 のアドレスがリースされます。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定した場合は、設定が削除されます。

<num>

- 割り当てアドレス数
  “4.1.3 lan ip dhcp service” の<mode>に server を指定した場合にだけ有効です。
  DHCP サーバサービスの場合に、割り当て可能な IP アドレスの総数を 1～64 の 10 進数値で指定します。
  省略した場合は、32 を指定したものとみなされます。

ホストデータベース機能を使用すると、特定の DHCP クライアントに対して固有の IP アドレスを割り当てることができます。この場合の IP アドレスは、割当て先頭 IP アドレスと割当てアドレス数によって規定される動的割り当て範囲である必要はありません。

<time>

- 割り当て時間

  DHCP クライアントに配布する情報の有効時間を、0 秒～365 日の範囲で指定します。

  単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。

  0 秒を指定した場合は、設定が削除され、有効時間監視なし (無限) とみなされます。

<gateway>

- デフォルトルータ IP アドレス

  DHCP クライアントに配布する、デフォルトルータの IP アドレスを設定します。

  0.0.0.0 を指定した場合は、設定が削除されます。

<domain>

- ドメイン名

  DHCP クライアントに配布するドメイン名を、0x21,0x23～0x7e の 80 文字以内の ASCII 文字列で指定します。なお、RFC1034 では英数字、”- ”(ハイフン)、”. ”(ピリオド) でドメイン名をつけることを推奨しています。

[説明]

DHCP サーバ機能を使用する場合に、クライアントに配布する情報を設定します。

[未設定時]

DHCP で配布される情報は設定されないものとみなされます。

4.1.5　lan ip route add

[機能]

IPv4 スタティックルーティング情報 (静的経路情報) の設定

[入力形式]

lan [<number>] ip route add <address> / <mask> <next_hop> [<metric> [<distance>]]

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<address>/<mask>

- IPv4 アドレス / マスクビット数 (またはマスク値)
  宛先ネットワークを IPv4 アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。
  - IPv4 アドレス / マスクビット数 (例: 192.168.1.0 / 24)
  - IPv4 アドレス / マスク値 (例: 192.168.1.0 / 255.255.255.0)
- default
  宛先ネットワークとしてデフォルトルートを設定する場合に指定します。
  0.0.0.0 / 0(0.0.0.0 / 0.0.0.0) を指定するのと同じ意味になります。

<next_hop>

- 中継ルータ IPv4 アドレス
  宛先ネットワークへパケットを送信するときの中継ルータの IPv4 アドレスを指定します。

<metric>

- RIP メトリック値
  このスタティックルーティング情報を RIP で広報する場合のメトリック値を、1〜15 の 10 進数値で指定します。
  省略した場合は、1 を指定したものとみなされます。
  RIP 広報メトリック値は、以下の計算式で決定されます。
  - RIP 広報メトリック値=出力インタフェースの設定メトリック値+1+<metric>

<distance>

- 優先度
  このスタティックルーティング情報の優先度を、0〜254 の 10 進数値で指定します。優先度は値が小さい方が高い優先度を示します。
  省略した場合は、0 を指定したものとみなされます。

[説明]

LAN インタフェースに対して、IPv4 スタティックルーティング (静的経路) を設定します。<distance>で設定した優先度は、IPv4 ルーティングプロトコルで受信した経路の優先度と比較され同じ経路の場合は優先度の高い方が選択されます。
IPv4 スタティックルーティング情報は、本装置全体で 64 個まで定義できます。

[注意]

<address>/<mask>がまったく同じ宛先に対し、1 つのスタティックルーティング情報が設定できます。

[未設定時]

IPv4 スタティックルーティング情報を設定しないものとみなされます。

4.1.6　lan ip route modify

[機能]

IPv4 スタティックルーティング情報 (静的経路情報) の修正

[入力形式]

lan [<number>] ip route modify <old_address>/<old_mask> <new_address>/<new_mask> <new_next_hop> [<new_metric> [<new_distance>]]

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<old_address>/<old_mask>

- IPv4 アドレス/マスクビット数 (またはマスク値)
  修正前の宛先ネットワークを IPv4 アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。
  - IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
  - IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)
- default
  修正前の宛先ネットワークにデフォルトルートを設定している場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<new_address>/<new_mask>

- IPv4 アドレス/マスクビット数 (またはマスク値)
  新しい宛先ネットワークを IPv4 アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。
  - IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
  - IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)
- default
  新しい宛先ネットワークとしてデフォルトルートを設定する場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<new_next_hop>

- 新しい中継ルータ IPv4 アドレス
  宛先ネットワークへパケットを送信するときの新しい中継ルータの IPv4 アドレスを指定します。

<new_metric>

- 新しいメトリック値
  新しいメトリック値を、1～15 の 10 進数値で指定します。
  省略した場合は、1 を指定したものとみなされます。

<new_distance>

- 新しい優先度
  新しい優先度を、0～254 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

[説明]

IPv4 スタティックルーティング情報を修正します。

4.1.7　lan ip route delete

[機能]

IPv4 スタティックルーティング情報 (静的経路情報) の削除

[入力形式]

lan [<number>] ip route delete <address> / <mask>

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<address>/<mask>

- IPv4 アドレス / マスクビット数 (またはマスク値)
  削除する宛先ネットワークを IPv4 アドレスとマスクビット数の組み合わせで指定します。
- default
  デフォルトルートを削除する場合に指定します。
  0.0.0.0 / 0(0.0.0.0 / 0.0.0.0) を指定するのと同じ意味になります。
- all
  すべてのスタティックルーティングを削除する場合に指定します。

[説明]

IPv4 スタティックルーティング情報を削除します。

4.1.8 lan ip rip

[機能]

ダイナミックルーティング情報 (RIP) の設定

[入力形式]

lan [<number>] ip rip <send> <receive> <metric> [<ignore> [<password>]]

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<send>

RIP の送信について指定します。

- v1
  RIPv1(Broadcast) を送信します。
- v2
  RIPv2(Broadcast) を送信します。
- v2m
  RIPv2(Multicast) を送信します。
- off
  RIP を送信しません。

<receive>

RIP の受信について指定します。

- v1
  RIPv1 を受信します。
- v2
  RIPv1, RIPv2 を受信します。
- off
  RIP を受信しません。

<metric>

- 加算メトリック値
  RIP 情報の加算メトリック値を、0〜16 の 10 進数値で指定します。
  RIP 広報メトリック値は、以下の計算式で決定されます。
  - RIP 広報メトリック値=RIP 受信パケットのメトリック値+1+<metric>

<ignore>

自装置に<password>を設定していないときに、パスワード付きの RIPv2 パケットを受信したときの破棄の動作を指定します。
省略した場合は、off を指定したものとみなされます。

- on
  受信した RIPv2 パケットを破棄します。
- off
  受信した RIPv2 パケットを破棄しません。

<password>

- RIPv2 パスワード
  <send>または<receive>に v2 を指定した場合のパスワードを、0x21,0x23～0x7e のコードで構成される 16 文字以内の ASCII 文字列で指定します。
  省略した場合は、パスワードなしとみなされます。

[説明]

LAN インタフェースに、IPv4 ダイナミックルーティング情報 (RIP) を設定します。
ダイナミックルーティングとはルータ間でルーティング情報をやりとりすることで、そのつど最適なルートを選択してデータ通信を行う方法です。

[未設定時]

IPv4 ダイナミックルーティング (RIP) を使用しないものとみなされます。

```
lan <number> ip rip off off 0 off
```

4.2 IPv6 関連情報

4.2.1 lan ip6 use

[機能]

IPv6 機能の設定

[入力形式]

lan [<number>] ip6 use <mode>

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<mode>

IPv6 パケットの送受信を行うかどうか指定します。

- on
  このインタフェースで、IPv6 パケットの送受信を行います。
- off
  このインタフェースで、IPv6 パケットの送受信を行いません。

[説明]

このインタフェースで、IPv6 機能を利用するかどうかを設定します。

[未設定時]

IPv6 機能を利用しないものとみなされます。

```
lan <number> ip6 use off
```

4.2.2　lan ip6 ifid

[機能]

IPv6 インタフェース ID の設定

[入力形式]

lan [<number>] ip6 ifid <interfaceID>

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<interfaceID>

このインタフェースで利用する ID を指定します。

- auto
  本装置が持つ MAC アドレスから、EUI-64 形式の ID を自動生成する場合に指定します。
- インタフェース ID
  このインタフェースで利用する ID を、16 進数値で指定します。4 桁ずつ":"(コロン) で区切ってください。なお、各フィールドの先頭の 0 は省略できます (例: 2a0:c9ff:fe84:759)。

通常は auto を指定してください。特定のインタフェース ID を指定する場合は、同一の link 上でホストと衝突しない値を指定してください。

[説明]

このインタフェースで利用する、インタフェース ID を設定します。

[未設定時]

インタフェース ID を自動生成するものとみなされます。

```
lan <number> ip6 ifid auto
```

4.2.3 lan ip6 address

[機能]

IPv6 アドレスの設定

[入力形式]

lan [<number>] ip6 address <count> <address>/<prefixlen> <valid> <preferred> [<flags>]

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<count>

- IPv6 アドレス定義番号
  IPv6 アドレスの定義番号を、0〜3 の 10 進数値で指定します。

<address>

- IPv6 アドレス
  128-bit の IPv6 アドレスを指定します。

<prefixlen>

- プレフィックス長
  IPv6 アドレスに対するプレフィックス長として、64 を指定します。

<valid>

- valid lifetime の時間
  このインタフェースから RA(Router Advertisement メッセージ) を送信するときに、このプレフィックスに対する valid lifetime を、0 秒〜365 日の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。
- infinity
  このインタフェースから RA を送信するときに、このプレフィックスに対する valid lifetime を無限とする場合に指定します。

<preferred>

- preferred lifetime の時間
  このインタフェースから RA を送信する場合に、このプレフィックスに対する preferred lifetime を、0 秒〜365 日の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。
  <preferred>は、<valid>よりも短い時間となるように設定してください。<preferred>が<valid>よりも大きい場合、<valid>と同じ時間として扱われます。
- infinity
  このインタフェースから RA を送信する場合に、このプレフィックスに対する preferred lifetime を無限とします。

<flags>

- RA Prefix Information に付与されるフラグ
  このインタフェースから RA を送出する場合に、この prefix に対する flags フィールドの値を 16 進数値で設定します。
  省略した場合は、c0 を指定したものとみなされます。

[説明]

このインタフェースにおける IPv6 アドレスを設定します。
<address>の指定において、<prefixlen>以降がすべて 0 の場合には、指定した値は IPv6 プレフィックスであると判断されます。この IPv6 プレフィックスとインタフェース ID によって、IPv6 アドレスが生成されます。

[未設定時]

Link local アドレス以外の IPv6 アドレスを設定しないものとみなされます。

4.2.4 lan ip6 address delete

[機能]

IPv6 アドレスの削除

[入力形式]

lan [<number>] ip6 address delete <count>

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<count>

- IPv6 アドレス定義番号
  削除する IPv6 アドレスの定義番号を指定します。
- all
  すべての IPv6 アドレスを削除する場合に指定します。

[説明]

IPv6 アドレスを削除します。

4.2.5　lan ip6 ra mode

[機能]

Router Advertisement の動作の設定

[入力形式]

lan [<number>] ip6 ra mode <mode>

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<mode>

- off
  RA の送信を行いません。
  定期送信、および host からの RS に対する RA の送信を行いません。
- send
  RA の送信を行います。
  定期送信、および host からの RS に対する RA の送信を行います。

[説明]

RA(Router Advertisement メッセージ) を送信するかどうかを設定します。

[未設定時]

RA の送信を行わないものとみなされます。

```
lan <number> ip6 ra mode off
```

4.2.6 lan ip6 ra interval

[機能]

Router Advertisement メッセージ送信間隔の設定

[入力形式]

lan [<number>] ip6 ra interval <max> <min> <lifetime>

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<max>

- 最大送信間隔
  RA を定期送信する場合の最大送信間隔 (秒) を、4～1800 の 10 進数値で設定します。

<min>

- 最小送信間隔
  RA を定期送信する場合の最小送信間隔 (秒) を、3～<max>× 3/4 の 10 進数値で設定します。

<lifetime>

- Router Lifetime の値
  送信する RA の Router Lifetime の値を、0 または<max>～9000 の 10 進数値で設定します。

[説明]

RA の送信間隔、および RA の Router Lifetime の値の設定を行います。RA は<min>～<max>でランダムに決定された間隔で定期送信されます。

[未設定時]

最大送信間隔に 600 秒、最小送信間隔に 200 秒、Router Lifetime の値に 1800 が設定されたものとみなされます。

```
lan <number> ip6 ra interval 600 200 1800
```

4.2.7　lan ip6 ra mtu

[機能]

Router Advertisement メッセージに含める MTU option の設定

[入力形式]

lan [<number>] ip6 ra mtu <mtu>

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<mtu>

- MTU option の内容
  RA に含める MTU option の値を、0 または 1280～1500 の 10 進数値で設定します。
  0 を指定した場合は、RA に MTU option を含めません。

[説明]

RA に含める MTU option の値を設定します。

[未設定時]

送信する RA に MTU option を含めないものとみなされます。

```
lan <number> ip6 ra mtu 0
```

4.2.8 lan ip6 ra reachabletime

[機能]

Router Advertisement メッセージに含める Reachable Time の設定

[入力形式]

lan [<number>] ip6 ra reachabletime <reachabletime>

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<reachabletime>

- Reachable Time の値
  RA に含める Reachable Time の値を、0～3600000 の 10 進数値で設定します。

[説明]

RA に含める Reachable Time の値を設定します。

[未設定時]

Reachable Time の値として 0 が設定されたものとみなされます。

```
lan <number> ip6 ra reachabletime 0
```

4.2.9　lan ip6 ra retranstimer

[機能]

Router Advertisement メッセージに含める Retrans Timer の設定

[入力形式]

lan [<number>] ip6 ra retranstimer <retranstimer>

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<retranstimer>

- Retrans Timer の値
  RA に含める Retrans Timer の値を、0～4294967295 の 10 進数値で設定します。

[説明]

RA に含める Retrans Timer の値を設定します。

[未設定時]

Retrans Timer の値として 0 が設定されたものとみなされます。

```
lan <number> ip6 ra retranstimer 0
```

4.2.10 lan ip6 ra curhoplimit

[機能]

Router Advertisement メッセージに含める Cur Hop Limit の設定

[入力形式]

lan [<number>] ip6 ra curhoplimit <curhoplimit>

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<curhoplimit>

- Cur Hop Limit の値
  RA に含める Cur Hop Limit の値を、0～255 の 10 進数値で設定します。

[説明]

RA に含める Cur Hop Limit の値を設定します。

[未設定時]

Cur Hop Limit の値として 64 が設定されたものとみなされます。

```
lan <number> ip6 ra curhoplimit 64
```

4.2.11　lan ip6 ra flags

[機能]

Router Advertisement メッセージに含める flags field の設定

[入力形式]

lan [<number>] ip6 ra flags <flags>

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<flags>

- flags field の値
  RA に含める flags field の値を、00～ff の 16 進数値で設定します。

[説明]

RA に含める flags field の値を設定します。

[未設定時]

flags field の値として 00 が設定されたものとみなされます。

```
lan <number> ip6 ra flags 00
```

4.2.12 lan ip6 route add

[機能]

IPv6 スタティックルーティング情報 (静的経路情報) の設定

[入力形式]

lan [<number>] ip6 route add <address>/<prefixlen> <next_hop> [<metric>]

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<address>/<prefixlen>

- IPv6 アドレス/プレフィックス
  宛先ネットワークを IPv6 アドレスとプレフィックスの組み合わせを指定します。
- default
  宛先ネットワークとしてデフォルトルートを設定する場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<next_hop>

- 中継ルータ IPv6 アドレス
  宛先ネットワークへパケットを送信するときの中継ルータの IPv6 アドレスを指定します。
  ICMPv6redirect を正常に動作させるため、link-local address を指定してください。また、中継ルータが存在するネットワーク設定側に対して、適切にスタティックルートを設定してください。

<metric>

- メトリック値
  このスタティックルーティング情報を RIPng で広報する場合のメトリック値を、1〜15 の 10 進数値で指定します。
  省略した場合は、1 を指定したものとみなされます。
  RIPng 広報メトリック値は、以下の計算式で決定されます。
  - RIPng 広報メトリック値=出力インタフェースの設定メトリック値+1+<metric>

[説明]

IPv6 スタティックルーティング情報 (静的経路情報) を設定します。
IPv6 スタティックルーティング情報は、本装置全体で 64 個まで定義できます。

[未設定時]

IPv6 スタティックルーティング情報を設定しないものとみなされます。

4.2.13　lan ip6 route modify

[機能]

IPv6 スタティックルーティング情報 (静的経路情報) の修正

[入力形式]

lan [<number>] ip6 route modify <old_address>/<old_prefixlen> <new_address>/<new_prefixlen> <new_next_hop> [<new_metric>]

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<old_address>/<old_prefixlen>

修正前の IPv6 アドレスとプレフィックスの組み合わせを指定します。

- IPv6 アドレス/プレフィックス
  すでに定義されている宛先ネットワークの IPv6 アドレスとプレフィックスの組み合わせを指定します。
- default
  宛先ネットワークとしてデフォルトルートを登録する場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<new_address>/<new_prefixlen>

新しい IPv6 アドレスとプレフィックスの組み合わせを指定します。

- IPv6 アドレス/プレフィックス長
  新しい宛先ネットワークの IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- default
  宛先ネットワークとしてデフォルトルートを登録する場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<new_next_hop>

- 新しい中継ルータ IPv6 アドレス
  宛先ネットワークへパケットを送信する場合の、中継ルータ IPv6 アドレスを指定します。

<new_metric>

- 新しいメトリック値
  新しいメトリック値を、1〜15 の 10 進数値で指定します。
  省略した場合は、1 を指定したものとみなされます。

[説明]

IPv6 スタティックルーティング情報 (静的経路情報) を修正します。

4.2.14 lan ip6 route delete

[機能]

IPv6 スタティックルーティング情報 (静的経路情報) の削除

[入力形式]

lan [<number>] ip6 route delete <address>/<prefixlen>

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<address>/<prefixlen>

削除する IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長
  削除する IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- all
  すべてのスタティックルーティングを削除する場合に指定します。

[説明]

IPv6 スタティックルーティング情報 (静的経路情報) を削除します。

4.2.15　lan ip6 ripng

[機能]

ダイナミックルーティング情報 (RIPng) の設定

[入力形式]

lan [<number>] ip6 ripng <send> <receive> [<site> [<metric>]]

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<send>

RIPng パケットを定期送信するかどうか指定します。

- on
  RIPng パケットを定期送信します。
- off
  RIPng パケットを定期送信しません。

<receive>

RIPng パケットを受信するかどうか指定します。

- on
  RIPng パケットを受信します。
- off
  RIPng パケットを受信しません。

<site>

site-local prefix を送受信するかどうか指定します。

- on
  site-local prefix を送受信します。
- off
  site-local prefix を送受信しません。

<send>および<receive>に off を指定した場合は、本パラメタにも off を指定してください。
省略した場合は、off を指定したものとみなされます。

<metric>

- 加算メトリック値
  RIPng 情報の加算メトリック値を、0〜16 の 10 進数値で指定します。
  <send>に off を指定した場合は省略できます。
  省略した場合は、0 を指定したものとみなされます。
  RIPng 広報メトリック値は、以下の計算式で決定されます。
  - RIPng 広報メトリック値=RIPng 受信パケットのメトリック値+1+<metric>

[説明]

このインタフェースでの IPv6 ダイナミックルーティングの動作を設定します。

[未設定時]

IPv6ダイナミックルーティング機能を使用しないものとみなされます。

```
lan <number> ip6 ripng off off off 0
```

4.2.16　lan ip6 aggregate

[機能]

ダイナミックルーティング情報 (RIPng) における経路集約の設定

[入力形式]

lan [<number>] ip6 aggregate <count> <address>/<prefixlen> <rejectroute>

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 集約経路定義番号
  集約経路の定義番号を、0〜3 の 10 進数値で指定します。

<address>/<prefixlen>

- IPv6 アドレス/プレフィックス長
  集約経路の宛先ネットワークを IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- default
  集約経路としてデフォルトルートを登録する場合に指定します。::/0 を指定するのと同じ意味になります。

<rejectroute>

- on
  集約経路に対する破棄経路を設定します。
- off
  集約経路に対する破棄経路を設定しません。

[説明]

RIPng における集約経路の設定を行います。
集約経路が設定された場合には、設定された集約経路に含まれる個々の経路は広報されず、集約経路だけを広報します。また、集約経路と等しいネットワークに対する経路情報を持たない場合には、実際に持たない宛先に対するパケットを破棄するために、設定された集約経路に対する破棄経路を設定することもできます。
同一 lan 定義内に同一の集約経路は設定できません。

[未設定時]

経路集約は行わないものとみなされます。

4.2.17　lan ip6 aggregate delete

[機能]

ダイナミックルーティング情報 (RIPng) における経路集約の削除

[入力形式]

lan [<number>] ip6 aggregate delete <count>

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 集約経路定義番号
  削除する集約経路の定義番号を、0〜3 の 10 進数値で指定します。
- all すべての集約経路を削除する場合に指定します。

[説明]

集約経路の削除を行います。

4.3　ブリッジ関連情報

4.3.1　lan bridge use

[機能]

ブリッジ動作モード の設定

[入力形式]

lan [<number>] bridge use <mode>

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<mode>

ブリッジを使用するかどうかを指定します。

- on
  ブリッジを使用する場合に指定します。
- off
  ブリッジを使用しない場合に指定します。

[説明]

ブリッジを使用するかどうかを設定します。
ブリッジを使用する場合、IP および IPv6 のパケット以外をすべてブリッジします。

[注意]

IP および IPv6 以外のネットワークプロトコル (IPX など) をルーティングしているネットワークでブリッジを使用する場合は、ブリッジによって中継されることでネットワークがダウンすることがあります。ルーティングと併用する場合は、ルーティングによって転送するプロトコルをフィルタリングするように設定してください。

[未設定時]

ブリッジを使用しないものとみなされます。

```
lan <number> bridge use off
```

4.3.2 lan bridge stp use

[機能]

STP 動作モード の設定

[入力形式]

lan [<number>] bridge stp use <mode>

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<mode>

- on
  STP を使用する場合に指定します。
- off
  STP を使用しない場合に指定します。

[説明]

スパニングツリーアルゴリズムで経路制御を行うかどうかを設定します。
本コマンドは、ブリッジを使用している場合にだけ有効です。

[未設定時]

STP を使用しないものとみなされます。

```
lan <number>  bridge stp use off
```

4.3.3　lan bridge stp cost

[機能]

パスコストの設定

[入力形式]

lan [<number>] bridge stp cost <path_cost>

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<path_cost>

LAN を経由する通信のパスコストを指定します。

- auto
  インタフェースの速度に応じて、パスコストが自動決定されます。
  以下に、本パラメタ指定時のパスコストを示します。

回線種別	パスコスト
Ethernet(10Mbps)	100
HSD(64kbps)	15620
HSD(128kbps)	7810
FR(64kbps)	16000
FR(128kbps)	8500
ISDN(64kbps)	16000

- パスコスト
  パスコストを、1〜65535 の 10 進数値で指定します。値が小さいほど、優先度が高くなります。

通常は auto を指定してください。ただし、ブリッジネットワークを構築するうえで、優先ブリッジ決定のために任意のパスコストを指定することができます。

[説明]

スパニングツリーアルゴリズムで使用するパスコストを設定します。
本コマンドは、STP を使用する場合にだけ有効です。

[未設定時]

パスコストを自動決定するとみなされます。

```
lan <number> bridge stp cost auto
```

4.3.4 lan bridge stp priority

[機能]

インタフェース優先度の設定

[入力形式]

lan [<number>] bridge stp priority <port_priority>

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<port_priority>

- インタフェース優先度
  インタフェースごとの優先度を、0～255 の 10 進数値で指定します。値が小さいほど、優先度が高くなります。

[説明]

スパニングツリーアルゴリズムで使用する、インタフェースごとの優先度を設定します。
本コマンドは、STP を使用する場合にだけ有効です。
本コマンドを設定しない場合は、<number>で指定したインタフェースが優先となり、remote 定義で定義されたインタフェースが非優先となります。lan 定義内で定義されたインタフェースでは、定義番号のもっとも小さいものが優先されます。

[未設定時]

インタフェース優先度に 128 が設定されたものとみなされます。

```
lan <number> bridge stp priority 128
```

4.4　VRRP 関連情報

4.4.1　lan vrrp use

[機能]

VRRP 動作モード の設定

[入力形式]

lan [<number>] vrrp use <mode>

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<mode>

VRRP 機能を使用するかどうかを指定します。

- on
  VRRP を使用する場合に指定します。
  <number>で指定した LAN インタフェースで VRRP が機能します。
- off
  VRRP を使用しない場合に指定します。
  <number>で指定した LAN インタフェースで VRRP は機能しません。

[説明]

この LAN インタフェースで、VRRP 機能を使用するかどうかを設定します。
VRRP 機能を使用しないと設定した場合、<number>で指定した LAN インタフェースでは VRRP 機能が動作しません。

[未設定時]

VRRP 機能を使用しないものとみなされます。

```
lan <number> vrrp use off
```

4.4.2 lan vrrp auth

[機能]

VRRP-AD の認証方法と認証パスワード の設定

[入力形式]

lan [<number>] vrrp auth <method> [<password>]

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<method>

認証方法について指定します。

- none
  <number>で指定した LAN インタフェースで VRRP-AD の認証を行いません。
- text
  <number>で指定した LAN インタフェースはテキスト パスワード を用いて VRRP-AD の認証を行います。

<password>

- 認証パスワード
  <method>に text を指定した場合、<number>で指定した LAN インタフェースで使用する VRRP-AD の認証パスワード を、0x21,0x23 ～ 0x7e の 8 桁以内の ASCII 文字列で指定します。

[説明]

この LAN インタフェースで VRRP-AD の認証に使用する認証方法と認証パスワード を設定します。
設定はこの LAN インタフェースに関係する VRRP グループのすべてに適用されます。
<method>に text を指定した場合は、パスワード を設定する必要があります。<method>に none を指定した場合、パスワード は指定できません。

[未設定時]

VRRP-AD の認証を使用しないものとみなされます。

```
lan <number> vrrp auth none
```

4.4.3　lan vrrp group id

[機能]

VRRP グループの設定

[入力形式]

lan [<number>] vrrp group <vrrp_number> id <vrid> <priority> [<virtual_ip#1> [<virtual_ip#2>]]

[パラメタ]

<number>

- lan 定義番号

  lan 定義番号として、0 を指定してください。

  省略した場合は、0 を指定したものとみなされます。

<vrrp_number>

- VRRP グループ定義番号

  LAN インタフェースに対する VRRP グループ定義の通し番号を、0～1 の 10 進数値で指定します。

<vrid>

- VRID

  <vrrp_number>で定義した VRRP グループの保持する VRID を、1～255 の 10 進数値で指定します。

  VRID は装置内で一意でなければなりません。重複した VRID を指定した場合は<number>および<vrrp_number>の最小である設定のみが有効となり、ほかはすべて無効となります。

<priority>

- VRRP ルータの優先度

  VRRP ルータの優先度を、"master"、または 1～254 の 10 進数値で指定します。<priority>に"master"を指定した場合、VRRP グループは優先度 255 のマスタルータとして動作します。この場合、仮想ルータの IPv4 アドレスは<number>で指定した LAN インタフェースの実 IPv4 アドレスになります。

  lan <number> ip address <address> / <mask> <broadcast> で設定された<address>が実 IPv4 アドレスです。

  また、この場合には lan vrrp group preempt の指定は無効になり、プリエンプトモードは常に ON で動作します。

  それ以外の場合、VRRP グループは<priority>で指定した優先度のバックアップルータとして動作します。

<virtual_ip#X>

- 仮想ルータの IPv4 アドレス

  VRRP グループで使用する仮想ルータの IPv4 アドレスを指定します。アドレス"0.0.0.0"または"255.255.255.255"は指定不可です。

  <priority>に"master"を指定した場合は、仮想ルータの IPv4 アドレスは<number>で指定した LAN インタフェースの実 IPv4 アドレスとなるため、指定することはできません。このときセカンダリ IPv4 アドレスが設定されている場合はセカンダリ IPv4 アドレスも仮想ルータの IPv4 アドレスとなります。

  lan <number> ip alias <address> / <mask> <broadcast> で設定された<address>がセカンダリ IPv4 アドレスです。

  それ以外の場合は、1 つ以上の仮想ルータの IPv4 アドレスを指定しなければなりません。また、その場合は VRRP グループ内で重複した仮想ルータの IPv4 アドレスを設定することはできません。仮想ルータの IPv4 アドレスに装置内のインタフェース実 IPv4 アドレスまたは、セカンダリ IPv4 アドレスを指定した場合は、この VRRP グループは無効となります。

[説明]

VRRP グループの VRID、優先度、仮想ルータの IPv4 アドレスを設定します。
マスタルータの設定は VRRP グループにつき 1 台の VRRP ルータにのみ行ってください。複数のマスタルータを設定した場合、仮想ルータを正しくバックアップすることができません。(VRRP グループで同一の仮想ルータの IPv4 アドレスが設定できないため。)
VRRP グループは VRID によって識別される同一 VRRP グループ内で優先度を競合し、マスタルータを決定します。
VRRP グループの仮想 MAC アドレスは VRID から自動的に生成されます。(00:00:5E:00:01:{VRID}) バックアップルータとして優先度を設定した場合でも、指定した優先度が同一 VRRP グループ内でもっとも高い優先度であればマスタルータとして動作します。また、VRRP ルータの優先度は VRRP グループ内で、できるだけ大きな差がつくように設定してください。近い優先度であった場合、マスタルータの切り替わりがスムーズに行われない場合があります。
VRRP 機能を使用する場合、本定義は必須定義であり未設定の場合は VRRP 機能が動作しません。

[未設定時]

VRRP グループの情報は設定されないものとみなされます。

4.4.4　lan vrrp group ad

[機能]

VRRP-AD の設定

[入力形式]

lan [<number>] vrrp group <vrrp_number> ad <interval>

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<vrrp_number>

- VRRP グループ定義番号
  LAN インタフェースに対する VRRP グループ定義の通し番号を、0〜1 の 10 進数値で指定します。

<interval>

- VRRP-AD 送出間隔
  VRRP-AD の送出間隔を、1 秒〜255 秒の範囲で指定します。単位は、m(分)、s(秒) のいずれかを指定します。

[説明]

該当する自装置 VRRP グループが使用する VRRP-AD の送信間隔時間を設定します。
同一 VRRP グループ内では送出間隔時間を同じ値に設定してください。異なる値が設定された場合はスムーズにマスタルータの交代が行われなくなる可能性があります。

[未設定時]

VRRP-AD の送出間隔として 1 秒が設定されたものとみなされます。

```
lan <number> vrrp group <vrrp_number> ad 1s
```

4.4.5 lan vrrp group preempt

[機能]

プリエンプトモードの設定

[入力形式]

lan [<number>] vrrp group <vrrp_number> preempt <mode> [<time>]

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<vrrp_number>

- VRRP グループ定義番号
  LAN インタフェースに対する VRRP グループ定義の通し番号を、0～1 の 10 進数値で指定します。

<mode>

プリエンプトモードを指定します。

- on
  <vrrp_number>で指定した VRRP グループでプリエンプトモードを ON に設定します。
- off
  <vrrp_number>で指定した VRRP グループでプリエンプトモードを OFF に設定します。

<time>

- プリエンプトモード OFF への移行禁止時間
  VRRP が動作を開始してから、プリエンプトモード OFF へ移行するのを禁止する時間として 0 秒～900 秒の範囲で指定します。
  単位は、m(分)、s(秒) のいずれかを指定します。
  省略した場合は、0 秒を指定したものとみなされます。
  なお、<mode>が off に設定されている場合にのみ有効であり、<mode>が on に設定される場合は指定できません。
  禁止時間内ではプリエンプトモードが ON に設定されたのと同様に動作します。この設定はシステム起動時に優先度の低いルータが先に動作を開始して、優先度の高いルータにマスタルータが渡されないようなことが発生する場合に有効です。

[説明]

VRRP グループのプリエンプトモードを設定します。

[未設定時]

プリエンプトモードに ON が設定されたものとみなされます。

```
lan <number> vrrp group <vrrp_number> preempt on
```

4.4.6　lan vrrp group trigger ifdown

[機能]

インタフェーストリガイベントの設定

[入力形式]

lan [<number>] vrrp group <vrrp_number> trigger <trigger_no> ifdown <interface> [<priority>]

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<vrrp_number>

- VRRP グループ定義番号
  LAN インタフェースに対する VRRP グループ定義の通し番号を、0～1 の 10 進数値で指定します。

<trigger_no>

- トリガイベント定義番号
  VRRP グループに対するトリガイベント定義の通し番号を、0～49 の 10 進数値で指定します。

<interface>

トリガイベント対象インタフェースを指定します。

- インタフェース名
  rmt0～rmt47 の範囲で指定します。
- any
  ループバックインタフェース以外すべてのパケット送出インタフェースをトリガイベント対象に含める場合に指定します。

<priority>

- 優先度
  変化させる優先度を、1～254 の 10 進数値で指定します。
  省略した場合は、254 を指定したものとみなされます。

[説明]

インタフェーストリガイベントを設定します。
<interface>で指定したインタフェースがダウンした場合、トリガイベントを適用します。
<interface>で指定したインタフェースが有効ではないインタフェースであった場合はトリガイベントは動作しません。また、同一インタフェースに重複してトリガイベントが設定された場合はすべてを適用します。
<interface>がリモートインタフェースである場合、ケーブル抜け、同期はずれ、または PVC 状態確認手順によって通信不可と判断された該当インタフェースに設定されたトリガイベントを適用します。
トリガイベントが適用された場合、VRRP グループの現在の優先度から<priority>で指定した値を減算した優先度の VRRP ルータとして動作します。
<priority>で優先度を減算すると 1 以下になる場合は、優先度 1 の VRRP ルータとして動作します。

[注意]

HUB である LAN インタフェース、または物理インタフェース以外を<interface>に指定してもインタフェーストリガイベントは動作しません。

[未設定時]

インタフェーストリガイベントは設定されないものとみなされます。

4.4.7　lan vrrp group trigger route

[機能]

ルートダウントリガイベントの設定

[入力形式]

lan [<number>] vrrp group <vrrp_number> trigger <trigger_no> route <dst_addr> <interface> [<priority>]

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<vrrp_number>

- VRRP グループ定義番号
  LAN インタフェースに対する VRRP グループ定義の通し番号を、0〜1 の 10 進数値で指定します。

<trigger_no>

- トリガイベント定義番号
  VRRP グループに対するトリガイベント定義の通し番号を、0〜49 の 10 進数値で指定します。

<dst_addr>

トリガイベントを適用する経路を指定します。

- IPv4 アドレス/マスクビット数 (またはマスク値)
  宛先または中継先ネットワークの IPv4 アドレスとマスクビット数の組み合わせを指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。
  以下に、有効な記述形式を示します。
  - IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
  - IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)

  設定値として、0.0.0.0 は指定できません。
- default
  経路としてデフォルトルートを指定します。

<interface>

トリガを適用する経路のパケット送出インタフェースを指定します。

- インタフェース名
  lan0 または rmt0〜rmt47 の範囲で指定します。
- any
  パケット送出インタフェースを特定しない場合に指定します。

<priority>

- 優先度
  変化させる優先度を、1〜254 の 10 進数値で指定します。
  省略した場合は、254 を指定したものとみなされます。

[説明]

ルートダウントリガイベントを設定します。
<dst_addr>で指定した宛先のパケットを<interface>で指定したインタフェースに送出する経路がルーティングテーブルに存在しない場合、トリガイベントを適用します。<interface>が any である場合は、送出先インタフェースに関係なく宛先の経路が存在していればトリガイベントは適用となりません。
トリガイベントが適用された場合、VRRP グループの現在の優先度から<priority>で指定した値を減算した優先度の VRRP ルータとして動作します。
<priority>で優先度を減算すると 1 以下になる場合は、優先度 1 の VRRP ルータとして動作します。
なお、VRRP グループが設定された LAN インタフェースがダウンした場合はこの限りではありません (自装置の VRRP グループは仮想ルータとして無効な状態となります)。

[未設定時]

ルートダウントリガイベントを設定しないものとみなされます。

4.4.8　lan vrrp group trigger node

[機能]

ノードトリガイベントの設定

[入力形式]

lan [<number>] vrrp group <vrrp_number> trigger <trigger_no> node <dst_addr> <interface> [<priority> [<resend_time> [<time_out> [<normal_interval> [error_interval>]]]]]

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<vrrp_number>

- VRRP グループ定義番号
  LAN インタフェースに対する VRRP グループ定義の通し番号を、0〜1 の 10 進数値で指定します。

<trigger_no>

- トリガイベント定義番号
  VRRP グループに対するトリガイベント定義の通し番号を、0〜49 の 10 進数値で指定します。

<dst_addr>

- ICMP ECHO パケットの宛先 IP アドレス
  ICMP ECHO パケットの宛先 IP アドレスを指定します。

<interface>

ICMP ECHO パケットを送出するインタフェースを指定します。

- インタフェース名
  rmt0〜rmt47 の範囲で指定します。
- any
  パケット送出インタフェースを特定しない場合に指定します。

<priority>

- 優先度
  変化させる優先度を、1〜254 の 10 進数値で指定します。
  省略した場合は、254 を指定したものとみなされます。

<resend_time>

- ICMP ECHO パケットの再送間隔
  ICMP ECHO パケットの再送間隔を、1 秒〜60 秒の範囲で指定します。
  単位は、m(分)、s(秒) のいずれかを指定します。
  省略した場合は、5 秒を指定したものとみなされます。

<time_out>

- ICMP ECHO のタイムアウト時間
  ICMP ECHO のタイムアウト時間を、<resend_time>+1 秒〜240 秒の範囲で指定します。
  単位は、m(分)、s(秒) のいずれかを指定します。
  省略した場合は、<resend_time>× 3 ＋ 1 秒を指定したものとみなされます。

<normal_interval>

- ICMP ECHO パケットの正常時送信間隔
  ICMP ECHO パケットの正常時送信間隔を、<time_out>+1 秒～255 秒の範囲で指定します。単位は、m(分)、s(秒) のいずれかを指定します。
  省略した場合は、<time_out>+1 秒を指定したものとみなされます。

<error_interval>

- ICMP ECHO パケットの異常時送信間隔
  ICMP ECHO パケットの異常時送信間隔を、1 秒～255 秒の範囲で指定します。
  単位は、m(分)、s(秒) のいずれかを指定します。
  省略した場合は、30 秒を指定したものとみなされます。

[説明]

ノードトリガイベントを設定します。
<dst_addr>で指定した宛先に ICMP ECHO パケットを<interface>で指定したインタフェースから送出し、<time_out>時間応答がない場合、トリガイベントを適用します。<interface>が any である場合、送出先インタフェースは経路情報に依存します。
トリガイベントが適用された場合、VRRP グループの現在の優先度から<priority>で指定した値を減算した優先度の VRRP ルータとして動作します。
<priority>で優先度を減算すると 1 以下になる場合は、優先度 1 の VRRP ルータとして動作します。
なお、VRRP グループが設定された LAN インタフェースがダウンした場合はこの限りではありません (自装置の VRRP グループは仮想ルータとして無効な状態となります)。

[注意]

<dst_addr>にはブロードキャストアドレス、マルチキャストアドレスを指定しないでください。指定した場合は正常に動作しません。
優先度を"master"に設定した VRRP グループにノードトリガを設定した場合は正常に動作しません。ノードトリガを設定する場合は優先度を"master"以外にしてください。
ノードトリガで送信される ICMP ECHO パケットの送信元 IP アドレスは VRRP グループが設定された LAN のインタフェースアドレスとなりますので、ICMP ECHO 応答パケットの経路に注意してください。
ノードトリガでは定期的にパケットが送信されますので異常課金に注意してください。

[未設定時]

ノードトリガイベントは設定されないものとみなされます。

4.4.9　lan vrrp group trigger delete

[機能]

トリガイベントの削除

[入力形式]

lan [<number>] vrrp group <vrrp_number> trigger delete <trigger_no>

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<vrrp_number>

削除するトリガが設定された VRRP グループを指定します。

- VRRP グループ定義番号
  LAN インタフェースに対する VRRP グループ定義の通し番号を、0～1 の 10 進数値で指定します。

<trigger_no>

削除するトリガイベントを指定します。

- トリガイベント定義番号
  削除するトリガイベント定義の通し番号を、0～49 の 10 進数値で指定します。
- all
  VRRP グループに対するすべてのトリガイベント定義を削除する場合に指定します。

[説明]

VRRP グループに対するトリガイベントを削除します。
VRRP グループを削除しても<vrrp_number>のソートはしません。

4.4.10 lan vrrp group delete

[機能]

VRRP グループの削除

[入力形式]

lan [<number>] vrrp group delete <vrrp_number>

[パラメタ]

<number>

- lan 定義番号
  lan 定義番号として、0 を指定してください。
  省略した場合は、0 を指定したものとみなされます。

<vrrp_number>

削除する VRRP グループを指定します。

- VRRP グループ定義番号
  削除する VRRP グループ定義の通し番号を、0～1 の 10 進数値で指定します。
- all
  すべての VRRP グループ定義を削除する場合に指定します。

[説明]

VRRP グループ定義番号で指定した VRRP グループ定義を削除します。

第 5 章　相手情報の設定

5.1　相手共通情報

5.1.1　remote delete

[機能]

相手ネットワークの削除

[入力形式]

remote delete <number>

[パラメタ]

<number>

削除する相手ネットワークを指定します。

- 相手定義番号
  削除する相手ネットワークの通し番号を指定します。
- all
  すべての相手ネットワークを削除する場合に指定します。

[説明]

相手ネットワークを削除します。

5.1.2 remote name

[機能]

相手ネットワーク名称の設定

[入力形式]

remote [<number>] name <network_name>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<network_name>

- 相手ネットワーク名
  相手ネットワーク名を、0x21,0x23～0x7e の 8 文字以内の ASCII 文字列で指定します。

[説明]

相手ネットワーク名を設定します。

[注意]

すでに同一名称の相手ネットワークが登録されている場合は、異常終了します。

[未設定時]

相手ネットワーク名を設定しないものとみなされます。

5.1.3　remote autodial

[機能]

自動ダイヤル可否の設定

[入力形式]

remote [<number>] autodial <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

自動的にダイヤルするかどうかを指定します。

- enable
  送信すべきパケットが発生した場合に、自動ダイヤルを行います。
- disable
  送信すべきパケットが発生しても、自動ダイヤルを行いません。

[説明]

指定した相手に対して、自動的にダイヤルするかどうかを設定します。

[注意]

“3.2.7 wan isdn autodial” で<mode>に disable を指定している場合は、自動ダイヤルを行えません。
自動ダイヤルを行う場合は、<mode>に enable を指定しておいてください。

[未設定時]

自動ダイヤルを行うものとみなされます。

```
remote <number> autodial enable
```

5.1.4 remote mtu

[機能]

送信パケット最大長 (MTU 値) の設定

[入力形式]

remote [<number>] mtu <mtu>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mtu>

- MTU 値
  MTU 値を、200〜1500 の 10 進数値で指定します。

[説明]

リモートに対して送信するパケットの MTU 値を設定します。
MTU 値を変更すると、このリモートに対して送信するパケットの最大長が変更されます。また、PPP ネゴシエーションにおいて相手 MRU 値、相手 MRRU 値が MTU 値まで小さくなることを許すようになります。

[未設定時]

MTU 値に 1500 を指定したものとみなされます。

```
remote <number> mtu 1500
```

5.1.5　remote shaping

[機能]

シェーピング機能の設定

[入力形式]

remote [<number>] shaping <mode> [<rate>]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

- on
  シェーピングを使用します。
- off
  シェーピングを使用しません。

<rate>

- 最大送出レート
  最大送出レートを、1k〜128k の範囲の 10 進数値と単位文字で指定します。
  10 進数値の末尾に k の単位文字を付与することで単位を指定できます。
  単位文字を付与しない場合、単位は Kbps となります。
  単位文字 k を付与した場合、単位は Kbps となります。
  1Kbps は 1000bps です。

[説明]

シェーピング機能について設定します。
<mode>が on の場合、<rate>で設定したレートに送信を抑制します。回線速度を上回る値を設定した場合には、実質的にシェーピングは機能しません。
<mode>が off の場合、<rate>は設定できません。

[未設定時]

シェーピングを使用しないものとみなされます。

```
remote <number> shaping off
```

5.2 アクセスポイント情報

5.2.1 remote ap name

[機能]

アクセスポイントの名称の設定

[入力形式]

remote [<number>] ap [<ap_number>] name <ap_name>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_name>

- アクセスポイント名
  アクセスポイント名を、0x22(ダブルクォーテーション) を除く [0x21-0x7e] の範囲のコードで構成される ASCII 文字列で指定します。指定範囲は、1〜8 文字です。

[説明]

アクセスポイント名を設定します。

[注意]

アクセスポイントの情報をすべて未設定時の値で使用する場合には必ずアクセスポイント名を設定してください。すべての値が未設定時値の場合にはアクセスポイントの情報は削除されます。

[未設定時]

アクセスポイント名を設定しないものとみなされます。

5.2.2　remote ap move

[機能]

アクセスポイントの優先順序の変更

[入力形式]

remote [<number>] ap move <ap_number> <new_ap_number>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- 対象アクセスポイント定義番号
  優先順序を変更するアクセスポイント定義番号を指定します。

<new_ap_number>

- 移動先アクセスポイント定義番号
  対象アクセスポイントを移動させる先のアクセスポイント定義番号を指定します。
  対象アクセスポイントは、ここで指定したアクセスポイントの前に移動されます。

[説明]

アクセスポイントの順序を変更します。

5.2.3 remote ap delete

[機能]

アクセスポイントの削除

[入力形式]

remote [<number>] ap delete <ap_number>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

削除するアクセスポイント定義番号を指定します。

- アクセスポイント定義番号
  削除するアクセスポイント定義番号を指定します。
- all
  すべてアクセスポイント定義番号を削除する場合に指定します。

[説明]

アクセスポイントを削除します。

5.2.4　remote ap datalink type

[機能]

パケット転送方法の設定

[入力形式]

remote [<number>] ap [<ap_number>] datalink type <type>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<type>

パケットの転送方式を指定します。

- physical
  bind 命令 (“5.2.5 remote ap datalink bind” を参照) によって決定された利用回線のデフォルトの転送方式を提供する場合に指定します。以下に各回線のデフォルトの転送方式を示します。

ISDN	PPP
HSD	PPP
FR	RFC2427 方式

- ip
  IPv6 over IPv4 tunnel を使用する場合に指定します。
- ipsec
  IPsec を使用する場合に指定します。
- discard
  このアクセスポイント利用時にはすべてのパケットが破棄されます。

[説明]

指定したアクセスポイントを利用してパケットを転送する場合の転送方式を設定します。

[未設定時]

転送方式として physical を設定するものとみなされます。

```
remote <number> ap 0 datalink type physical
```

5.2.5 remote ap datalink bind

[機能]

パケット転送回線の設定

[入力形式]

remote [<number>] ap [<ap_number>] datalink bind <kind> [<conf_number>]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<kind>

- wan
  wan 定義によって指定される回線を利用する場合に指定します。
- lan
  lan 定義によって指定される回線を利用する場合に指定します。

<conf_number>

- wan 定義または lan 定義の定義番号
  利用する wan 定義番号として 0、または lan 定義番号として 0 を指定します。

[説明]

指定したアクセスポイント定義を利用してパケットを転送する場合の回線を設定します。
本コマンドは、“5.2.4 remote ap datalink type” の<type>で physical を指定した場合にだけ有効です。

[注意]

本コマンドは設定はできますが、無効です。

[未設定時]

<kind>に wan を、<conf_nubmer>に 0 を指定するものとみなされます。

```
remote <number> ap 0 datalink bind wan 0
```

5.2.6　remote ap ip dns

[機能]

DNS サーバアドレスの設定

[入力形式]

remote [<number>] ap [<ap_number>] ip dns <dns>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<dns>

- DNS サーバアドレス
  接続先と接続するときに利用する DNS サーバのアドレスを指定します。
  ここでの指定によって、以下のように動作します。

  0.0.0.0　アドレスを自動取得するものとみなされます。

  255.255.255.255
  DNS サーバを使用しないものとみなされます。

  上記以外　設定したアドレスを、相手装置に通知します。

[説明]

指定したアクセスポイントと接続するときに利用する DNS サーバアドレスを設定します。
本コマンドによる設定情報は、以下の 2 つの場合に利用されます。

- ProxyDNS からの利用
  ProxyDNS 機能と併用する場合、接続先と接続中のときは、<dns>で設定したアドレスに対して ProxyDNS から DNS 問い合わせを行います。本コマンドによる設定情報がない場合は、IPCP 機能によって相手ルータから DNS サーバアドレスを取得します。
- 通信相手への DNS サーバアドレス通知
  接続先から IPCP 機能を用いて DNS サーバアドレス通知要求を受けた場合に、<dns>で設定した IP アドレスを通知します。本コマンドによる設定がない場合は通知しません。

[未設定時]

アドレスを自動取得するものとみなされます。

```
remote <number> ap 0 ip dns 0.0.0.0
```

5.2.7 remote ap multiroute port add

[機能]

ポートルーティング情報の設定

[入力形式]

remote [<number>] ap [<ap_number>] multiroute port add <port> <server_name>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<port>

- サービスポート番号
  ポートルーティングの対象となるサービスポート番号を、1～65535 の 10 進数値で指定します。複数指定することはできません。

<server_name>

- サーバホスト名
  ポートルーティングサービスを提供するサーバホスト名を、80 文字以内で指定します。

[説明]

ポートルーティングの対象とするポート番号を設定します。
本コマンドを実行した場合、条件に一致するパケットが指定したアクセスポイントに送信されます。
ポートルーティング情報は、本装置全体で 32 個まで定義できます。

[未設定時]

ポートルーティング情報を定義しないものとみなされます。

5.2.8　remote ap multiroute port delete

[機能]

ポートルーティング情報の削除

[入力形式]

remote [<number>] ap [<ap_number>] multiroute port delete <port>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<port>

削除するサービスポート番号を指定します。

- サービスポート番号
  削除するサービスポート番号を指定します。
- all
  すべてのサービスポート番号を削除する場合に指定します。

[説明]

ポートルーティング情報を削除します。

5.2.9 remote ap multiroute src

[機能]

ソースアドレスルーティング情報の設定

[入力形式]

remote [<number>] ap [<ap_number>] multiroute src <src_addr>/<mask>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<src_addr>/<mask>

- IP アドレス/マスクビット数 (またはマスク値)
  ソースアドレスルーティングの対象とする IP アドレスとマスクビット数の組み合わせを指定します。マスクビット数と組み合わせることで、複数のソース IP アドレスを対象とすることができます。なお、マスク値は、最上位ビットから 1 で連続した値にしてください。
  - IP アドレス/マスクビット数 (例: 192.168.1.1/24)
  - IP アドレス/マスク値 (例: 192.168.1.1/255.255.255.0)

[説明]

ソースアドレスルーティングの対象とする IP アドレスを設定します。

[注意]

本コマンドを実行した場合、<src_addr>/<mask>に適合するソース IP アドレスを持つパケットのみがこのアクセスポイントに送信されます。
すべての接続先に対してソースアドレスルーティングを設定している場合、本装置のファームウェア更新や通信確認 (ping コマンド実行) などは行えません。必ず 1 以上、ソースアドレスルーティングを行わない接続先を定義してください。

[未設定時]

ソースアドレスルーティング情報を定義しないものとみなされます。

5.2.10　remote ap multiroute src delete

[機能]

ソースアドレスルーティング情報の削除

[入力形式]

remote [<number>] ap [<ap_number>] multiroute src delete

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

[説明]

ソースアドレスルーティング情報を削除します。

5.2.11 remote ap limit charge

[機能]

課金累計制限の設定

[入力形式]

remote [<number>] ap [<ap_number>] limit charge <charge>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<charge>

- 課金累計上限
  課金累計の上限金額を、0～999999 の 10 進数値で指定します。
  0 を指定した場合は、上限を設定しません。

[説明]

指定したアクセスポイントに対する課金累計の上限値を設定します。
発信時に、アクセスポイントに対する課金累計が指定した上限値を超えていた場合は、このアクセスポイントに対する自動発信を行いません。次の優先度のアクセスポイントに対して処理を移します。

[未設定時]

課金累計の上限値を設定しないものとみなされます。

```
remote <number> ap <ap_number> limit charge 0
```

5.2.12　remote ap limit time

[機能]

接続時間累計制限の設定

[入力形式]

remote [<number>] ap [<ap_number>] limit time <time>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time>

- 接続時間累計上限
  接続時間累計の上限時間を、0 秒～999 時間の範囲で指定します。単位は、d(日)、h(時)、m(分)、s(秒)のいずれかを指定します。0 秒を指定した場合は、上限を設定しません。

[説明]

指定したアクセスポイントに対する接続時間累計の上限値を設定します。
発信時に、このアクセスポイントに対する接続時間累計が指定した上限値を超えていた場合は、このアクセスポイントに対する自動発信を行いません。次の優先度のアクセスポイントに対して処理を移します。

[未設定時]

接続時間累計の上限値を設定しないものとみなされます。

```
remote <number> ap <ap_number> limit time 0s
```

5.2.13 remote ap ppp auth type

[機能]

認証方法の設定

[入力形式]

remote [<number>] ap [<ap_number>] ppp auth type <authtype>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<authtype>

認証プロトコルのタイプを指定します。

- off
  認証を要求しない場合に指定します。
- pap
  PAP による認証を要求する場合に指定します。
- chap_md5
  MD5-CHAP による認証を要求する場合に指定します。
- any
  MD5-CHAP または PAP による認証を要求し、実際に利用する認証プロトコルはネゴシエーションによって決定する場合に指定します。

[説明]

接続時に要求する認証プロトコルのタイプを設定します。
ここでの設定は、着信し、かつ CLID 相手判定が行われた場合に有効となります。

[未設定時]

着信時の認証プロトコルに MD5-CHAP または PAP を用います。

```
remote <number> ap 0 called ppp auth type any
```

5.2.14　remote ap ppp auth send

[機能]

送信認証情報の設定

[入力形式]

remote [<number>] ap [<ap_number>] ppp auth send <id> <password> [encrypted]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<id>

- 認証 ID
  認証 ID を、0x21,0x23〜0x7e の文字で構成される 64 文字以内の文字列を指定します。"delete"は指定できません。

<password>

- 認証パスワード
  認証パスワードを、0x21,0x23〜0x7e の文字で構成される 64 文字以内の文字列を指定します。
  show コマンドで表示される暗号化された認証パスワード文字列を encrypted とともに指定することもできます。その場合、表示された文字列をそのまま正確に入力してください。文字列は 64 文字を超えていてもかまいません。
- 暗号化された認証パスワード
  show コマンドで表示される暗号化された認証パスワードを encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化認証パスワード指定
  <password>に暗号化された認証パスワードを設定する場合に指定します。

[説明]

指定したアクセスポイントに接続するときに送信する認証情報 (認証 ID およびパスワード) を設定します。

[注意]

認証 ID およびパスワードが設定されていない場合、接続相手からの認証要求を拒否します。
show コマンドでは、暗号化された認証パスワードが encrypted と共に表示されます。

[未設定時]

送信する認証情報を定義しないものとみなされます。

5.2.15 remote ap ppp auth send delete

[機能]

認証情報の削除

[入力形式]

remote [<number>] ap [<ap_number>] ppp auth send delete

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

[説明]

認証情報 (認証 ID およびパスワード) を削除します。

5.2.16　remote ap ppp auth receive

[機能]

受諾認証情報の設定

[入力形式]

remote [<number>] ap [<ap_number>] ppp auth receive <id> <password> [encrypted]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<id>

- 認証 ID
  認証 ID を、0x21,0x23～0x7e の文字で構成される 64 文字以内の文字列を指定します。"delete"は指定できません。

<password>

- 認証パスワード
  認証パスワードを、0x21,0x23～0x7e の文字で構成される 64 文字以内の文字列を指定します。
  show コマンドで表示される暗号化された認証パスワードを encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化認証パスワード指定
  <password>に暗号化された認証パスワードを設定する場合に指定します。

[説明]

認証プロトコル使用時に受諾する、認証情報 (認証 ID および認証パスワード) を設定します。

[注意]

show コマンドでは、暗号化された認証パスワードが encrypted と共に表示されます。

[未設定時]

受諾する認証情報を設定しないものとみなされます。

5.2.17 remote ap ppp auth receive delete

[機能]

受諾認証情報の削除

[入力形式]

remote [<number>] ap [<ap_number>] ppp auth receive delete

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

[説明]

認証プロトコル使用時に受諾する、認証情報 (認証 ID および認証パスワード) を削除します。

5.2.18　remote ap ppp mp use

[機能]

発信時の MP 利用の可否の設定

[入力形式]

remote [<number>] ap [<ap_number>] ppp mp use <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

MP を利用するかどうかを指定します。

- off
  MP を利用しない場合に指定します。
- on
  MP を利用する場合に指定します。

[説明]

発信時に MP を利用するかどうかを設定します。
着信時は、CLID 相手判定によって指定したアクセスポイントへの接続が決定された場合に、MP を利用するかどうかを設定します。

[未設定時]

MP を利用しないものとみなされます。

```
remote <number> ap 0 ppp mp use off
```

5.2.19 remote ap ppp mp bap use

[機能]

発信時の BAP/BACP 利用の可否の設定

[入力形式]

remote [<number>] ap [<ap_number>] ppp mp bap use <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

BAP/BACP を利用するかどうかを指定します。

- off
  BAP/BACP を利用しない場合に指定します。
- on
  BAP/BACP を利用する場合に指定します。

[説明]

MP を利用する場合に BAP/BACP を利用するかどうかを設定します。
着信時は、CLID 相手判定によってこのアクセスポイントへの接続が決定された場合に、BAP/BACP を利用するかどうかを設定します。

[未設定時]

BAP/BACP を利用しないものとみなされます。

```
remote <number> ap 0 ppp mp bap use off
```

5.2.20　remote ap dial number

[機能]

アクセスポイントの電話番号の設定

[入力形式]

remote [<number>] ap [<ap_number>] dial <count> number <dial_number> [<subaddress>]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

ダイヤル定義番号として、以下のいずれかを指定します。

- 0
- 1
- 2

<dial_number>

- 相手電話番号
  相手の電話番号を、0～9 の数字と、*、#、-、(、)、\の文字で構成される 32 桁以内の ASCII 文字列で指定します。

<subaddress>

- 相手サブアドレス
  相手のサブアドレスを、0x21,0x23～0x7e の文字で構成される 19 桁以内の ASCII 文字列で指定します。

[説明]

アクセスポイントの電話番号を設定します。

[未設定時]

アクセスポイントの電話番号を設定しないものとみなされます。

5.2.21 remote ap dial speed

[機能]

アクセスポイントの通信速度の設定

[入力形式]

remote [<number>] ap [<ap_number>] dial <count> speed <speed> [<carrier>]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

ダイヤル定義番号として、以下のいずれかを指定します。

- 0
- 1
- 2

<speed>

通信速度、通信手順を指定します。

- 64K
  同期 PPP 64Kbps の場合に指定します。
- PIAFS
  PIAFS(32Kbps) 接続の場合に指定します。
- PIAFS64K
  PIAFS(64Kbps) 接続の場合に指定します。

<carrier>

通信速度に "PIAFS64K" を指定した場合に通信事業者を指定します。省略した場合は、"docomo" を指定したものとみなされます。なお、通信速度に "PIAFS64K" 以外を指定した場合には、本パラメタを指定しないでください。

- docomo
  NTT DoCoMo の PIAFS(64Kbps) 接続の場合に指定します。
- ddip
  ウィルコム (旧 DDI Pocket) の PIAFS(64Kbps) 接続の場合に指定します。

[説明]

アクセスポイントの通信速度および通信手順を設定します。

[未設定時]

通信速度に 64kbps を指定したものとみなされます。

```
remote <number> ap 0 dial <count> speed 64K
```

5.2.22 remote ap dial delete

[機能]

アクセスポイントの電話番号および通信速度の削除

[入力形式]

remote [<number>] ap [<ap_number>] dial delete <count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

削除するダイヤル定義を指定します。

- ダイヤル定義番号
  削除する電話番号のダイヤル定義番号を、0～2 の範囲で指定します。
- all
  すべてのダイヤル定義を削除する場合に指定します。

[説明]

アクセスポイントの電話番号および通信速度を削除します。

[注意]

削除は、ダイヤル定義番号の単位で行われます。したがって、アクセスポイント電話番号 (“5.2.20 remote ap dial number” を参照) および通信速度 (“5.2.21 remote ap dial speed” を参照) の設定は同時に削除されます。

5.2.23　remote ap callback

[機能]

コールバック要求動作の設定

[入力形式]

remote [<number>] ap [<ap_number>] callback <mode> [<kind> <time> [<callback_number> [<subaddress>]]]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

- enable
  発信時にコールバックを要求します。
- disable
  発信時にコールバックを要求しません。

<kind>

- clid
  コールバック方式に「無課金方式」を指定します。
- cbcp
  コールバック方式に「CBCP 方式」を指定します。

<time>

- コールバック待ち時間
  コールバック要求が受理されたあと、相手からのコールバック応答着信を待つ時間を、0 秒～60 秒の範囲で指定します。
  単位は、m(分)、s(秒) のいずれかを指定します。

<callback_number>

- コールバック電話番号
  コールバック要求時に相手に伝える自側の電話番号を、0～9 の数字と、*、#、-、(、)、\の文字で構成される 32 桁以内の ASCII 文字列で指定します。

<subaddress>

- コールバックサブアドレス
  コールバック要求時に相手に伝える自側の電話番号に対するサブアドレスを、0x21, 0x23～0x7e の文字で構成される 19 桁以内の ASCII 文字列で指定します。

[説明]

このアクセスポイントに対して発信する際のコールバック要求動作を設定します。
<callback_number> および <subaddress> の設定はコールバック方式に「cbcp」を設定し、相手システムがコールバック要求側からの電話番号指定を許可した場合に有効です。

[未設定時]

発信時にコールバック要求しないものとみなされます。

```
remote <number> ap <ap_number> callback disable
```

5.2.24　remote ap called accept

[機能]

アクセスポイントからの着信許可の設定

[入力形式]

remote [<number>] ap <ap_number> called accept <incoming>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<incoming>

着信を許可するかどうかを指定します。

- enable
  着信を許可する場合に指定します。
- disable
  着信を許可しない場合に指定します。

[説明]

指定したアクセスポイントから送られてきたと判断されたデータに対して、着信を許可するかどうかを設定します。

[未設定時]

着信を許可するものとみなされます。

```
remote <number> ap 0 called accept enable
```

5.2.25 remote ap called clid

[機能]

CLID 相手判断利用の可否の設定

[入力形式]

remote [<number>] ap <ap_number> called clid <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

着信時に CLID 相手判定をするかどうかを指定します。

- enable
  着信時に CLID 相手判定をする場合に指定します。
- disable
  着信時に CLID 相手判定をしない場合に指定します。

[説明]

着信時に、相手電話番号を判定するかどうかを設定します。相手電話番号を判定することを、CLID 相手判定と呼びます。

- 以下の定義の相手電話番号を利用して、着信時に相手を判定します。

  1) “5.2.26 remote ap called number” による定義が存在する場合は、その定義の相手電話番号。
  2) 1) の定義が存在せず、“5.2.20 remote ap dial number” による定義が存在する場合は、その定義の相手電話番号。

- 本コマンドの<mode>で enable を指定した場合に上記の番号が発信者番号として通知されたときは、指定したアクセスポイントから着信したものとみなされます。

[未設定時]

着信時に、CLID 相手判定を行うものとみなされます。

```
remote <number> ap 0 called clid enable
```

5.2.26　remote ap called number

[機能]

CLID の設定

[入力形式]

remote [<number>] ap [<ap_number>] called number <called_number> [<subaddress>]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<called_number>

相手電話番号

- 相手電話番号
  相手の電話番号を、0～9 の数字と、*、#、-、(、)、\の文字で構成される 32 桁以内の ASCII 文字列で指定します。
- any
  着信時の CLID 相手判定に、"“5.2.20 remote ap dial number”"で設定した相手電話番号を使用する場合に指定します。

<subaddress>

- 相手サブアドレス
  相手のサブアドレスを、0x21,0x23～0x7e の文字で構成される 19 桁以内の ASCII 文字列で指定します。

[説明]

CLID 相手判定で、チェックする番号を設定します。

[未設定時]

着信時の CLID 相手判定に、"“5.2.20 remote ap dial number”"で設定された相手電話番号を使用します。

```
remote <number> ap 0 called number any
```

5.2.27 remote ap called callback

[機能]

コールバック応答動作の設定

[入力形式]

remote [<number>] ap [<ap_number>] called callback <mode> [<kind> <time> [<callback_number> [<subaddress>]]]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

- enable
  着信時にコールバックを行います。
- disable
  着信時にコールバックを行いません。

以下のパラメタは、<mode>が disable の場合は省略できます。

<kind>

- clid
  コールバック方式として「無課金方式」を指定します。
- cbcp
  コールバック方式として「CBCP 方式」を指定します。

<time>

- コールバック待ち時間
  コールバック要求着信を受理したあと、相手にコールバック応答発信を行うまでの待ち時間を、0 秒～60 秒の範囲で指定します。
  単位は、m(分)、s(秒) のいずれかを指定します。

<callback_number>

- コールバック電話番号
  コールバック要求着信を受理したあと、コールバック応答発信で利用する電話番号を、0～9 の 10 進数値と ( ) \ - # * の区切り文字で構成される 32 桁以内の ASCII 文字列で指定します。

<subaddress>

- コールバックサブアドレス
  コールバック応答発信で利用する電話番号に対するサブアドレスを、0x21,0x23～0x7e の文字で構成される 19 桁以内の ASCII 文字列で指定します。

[説明]

このアクセスポイントに着信を受けた場合のコールバック応答動作の設定を行います。
この設定は発信者番号 (CLID) で相手識別が行われた場合に利用します。
コールバック方式に「cbcp」を指定し、<callback_number> の指定を行った場合には、コールバック要求側からの電話番号指定を許可しません。

[未設定時]

着信時にコールバック応答動作を行わないものとみなされます。

```
remote <number> ap <ap_number> called callback disable
```

5.2.28 remote ap idle

[機能]

無通信監視タイマの設定

[入力形式]

remote [<number>] ap [<ap_number>] idle <time> [<direction>]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time>

- 無通信監視時間
  無通信監視時間を、0 秒～3600 秒の範囲で指定します。単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。0 秒を指定した場合は、監視を行いません。

<direction>

- 省略
  送信パケット、および受信パケットを通信監視の対象とします。
- send
  送信パケットのみを通信監視の対象とします。受信パケットは監視対象とはなりません。
- receive
  受信パケットのみを通信監視の対象とします。送信パケットは監視対象とはなりません。

[説明]

指定した接続先と接続したときの無通信監視時間を設定します。
<time>で設定された間、監視対象となるパケットがない場合に、無通信として回線を切断します。

[未設定時]

無通信監視を行わないものとみなされます。

```
remote [<number>] ap [<ap_number>] idle 0d
```

5.2.29　remote ap step

[機能]

平日昼間時間帯の課金単位時間の設定

[入力形式]

remote [<number>] ap [<ap_number>] step <time>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time>

- 課金単位時間
  平日昼間時間帯 (月〜金曜日 8:00〜19:00) の課金単位時間 (秒) の 10 倍の値を、0〜36000 の 10 進数値で指定します (例: 180 秒=1800、16.5 秒=165)。0 を指定した場合は、課金単位に応じた接続保持を行いません。

[説明]

ISDN 回線を利用して通信するときの平日昼間時間帯 (月〜金曜日 08:00〜19:00) の課金単位時間を設定します。課金単位時間を設定すると、無通信の場合でも接続時間が設定値の整数倍になるまで接続を保持します。

[注意]

課金単位時間を設定する場合、本装置の時刻を正しく設定してください。
祝日の料金には対応していません。

[未設定時]

課金単位時間を設定しないものとみなされます。

5.2.30 remote ap step2

[機能]

夜間・休日時間帯の課金単位時間の設定

[入力形式]

remote [<number>] ap [<ap_number>] step2 <time2>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time2>

- 課金単位時間
  夜間・休日時間帯 (月〜金曜日 19:00〜23:00)、土 / 日曜日 (08:00〜23:00) の課金単位時間 (秒) の 10 倍の値を、0〜36000 の 10 進数値で指定します (例: 180 秒=1800、16.5 秒=165)。

[説明]

ISDN 回線を利用して通信するときの夜間・休日時間帯 (月〜金曜日 19:00〜23:00、土 / 日曜日 08:00〜23:00) の課金単位時間を設定します。課金単位時間を設定すると、無通信の場合でも接続時間が設定値の整数倍になるまで接続を保持します。

[注意]

課金単位時間を設定する場合、本装置の時刻を正しく設定してください。
この設定は、"“5.2.29 remote ap step”"を設定した場合にのみ有効です。祝日の料金には対応していません。

[未設定時]

課金単位時間を設定していないものとみなされ、"remote ap step"で設定した値が使用されます。

5.2.31　remote ap step3

[機能]

深夜時間帯の課金単位時間の設定

[入力形式]

remote [<number>] ap [<ap_number>] step3 <time3>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time3>

- 課金単位時間
  深夜時間帯 (全日 23:00～08:00) の課金単位時間 (秒) の 10 倍の値を、0～36000 の 10 進数値で指定します (例: 180 秒=1800、16.5 秒=165)。

[説明]

ISDN 回線を利用して通信するときの深夜時間帯 (全日 23:00～08:00) の課金単位時間を設定します。課金単位時間を設定すると、無通信の場合でも接続時間が設定値の整数倍になるまで接続を保持します。

[注意]

課金単位時間を設定する場合、本装置の時刻を正しく設定してください。
この設定は、""5.2.29 remote ap step""を設定した場合にのみ有効です。祝日の料金には対応していません。

[未設定時]

課金単位時間を設定していないものとみなされ、""5.2.30 remote ap step2""で設定した値が使用されます。
この設定もない場合には、""5.2.29 remote ap step""で設定した値が使用されます。

5.2.32 remote ap keep

[機能]

テレホーダイ (回線接続保持) 機能の設定

[入力形式]

remote [<number>] ap [<ap_number>] keep <keep>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<keep>

回線接続保持の方式を設定します。

- on
  回線接続を保持します。
- off
  回線接続を保持しません。
- connect
  常時接続機能を使用します。

[説明]

回線接続保持の方式を設定します。
"on"のときには回線接続保持の方式として、テレホーダイ機能による制御を行います。
"connect"のときには回線接続保持の方式として、常時接続機能による制御を行います。

[未設定時]

回線接続保持機能を使用しないものとみなされます。

```
remote <number> ap 0 keep off
```

5.2.33　remote ap ipsec type

[機能]

IPsec 情報のタイプの設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec type <type>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<type>

IPsec 情報のタイプを設定します。

- off
  IPsec を使用しません。
- ike
  IPsec の Aggressive Mode を使用します。

[説明]

IPsec を使用するかどうかを設定します。
IPsec の Aggressive Mode を使用する場合は、以下の設定も行ってください。

- remote ap ipsec ike protocol
- remote ap ipsec ike range
- remote ap ipsec ike encrypt
- remote ap ipsec ike auth
- remote ap ipsec ike pfs
- remote ap ipsec ike lifetime
- remote ap ipsec ike newsa initiator
- remote ap ipsec ike newsa responder
- remote ap ike port
- remote ap ike shared key
- remote ap ike proposal encrypt
- remote ap ike proposal hash
- remote ap ike proposal pfs
- remote ap ike proposal lifetime
- remote ap ike retry

- remote ap ike idtype
- remote ap ike name local
- remote ap ike release
- remote ap ike initial
- remote ap ike sessionwatch

IPsec の Main Mode を使用する場合は、「10 VPN 情報の設定」を参照してください。

IPsec 区間について

IPsec 区間は、tunnel 利用時の自側の tunnel endpoint アドレスと tunnel 利用時の相手側の tunnel endpoint アドレスの定義で指定します。
自動鍵設定 (交換) の場合、事前に tunnel endpoint アドレスが決定しているときは指定してください。

tunnel endpoint アドレスの設定例

双方の IP アドレスが固定で決まっている場合:

- remote 0 ap 0 tunnel local 192.168.1.1
- remote 0 ap 0 tunnel remote 172.168.1.1

自側の tunnel endpoint アドレスが不定である場合:

- remote 0 ap 0 tunnel remote 172.168.1.1

IPsec 対象パケットについて

自動鍵設定 (交換) の場合は、<number>で設定された相手情報に range 指定があればその範囲の IP パケットが IPsec 対象となります。range 指定がなければ<number>で設定された相手情報を使用する IP パケットすべてが IPsec 対象となります。

[注意]

1 つの相手情報に対して複数のアクセスポイント情報が設定されている場合、先頭に設定されているアクセスポイント情報の IPsec 情報と IKE 情報が有効になります。

[未設定時]

IPsec を使用しないものとみなされます。

```
remote <number> ap <ap_number> ipsec type off
```

5.2.34　remote ap ipsec ike protocol

[機能]

自動鍵交換用 IPsec 情報のセキュリティプロトコルの設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike protocol <protocol>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<protocol>

自動鍵交換用 IPsec SA のセキュリティプロトコルを指定します。

- none
  セキュリティプロトコル未指定
- esp
  暗号
- ah
  認証

[説明]

自動鍵交換用 IPsec SA の、セキュリティプロトコルの設定を行います。

[未設定時]

自動鍵交換用 IPsec 情報のセキュリティプロトコルは未指定となります。

```
remote <number> ap <ap_number> ipsec ike protocol none
```

5.2.35 remote ap ipsec ike encrypt

[機能]

自動鍵交換用 IPsec 情報の暗号情報の設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike encrypt <enc_algo>[,<enc_algo>...]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<enc_algo>

暗号アルゴリズムを指定します。
複数のアルゴリズムを指定することができます。複数定義するときは、アルゴリズムを空白なしでカンマ','で区切ります。

- des-cbc
- 3des-cbc
- null
- none

[説明]

送受信パケットを暗号化／復号化するための、暗号アルゴリズムの設定を行います。
暗号鍵は自動生成されるので、設定は不要です。
暗号アルゴリズムを複数指定する場合、指定順序にかかわらず以下の優先順位となります。

1) 3des-cbc
2) des-cbc
3) null

[未設定時]

IPsec によるパケット暗号は行われません。

```
remote <number> ap <ap_number> ipsec ike encrypt none
```

5.2.36　remote ap ipsec ike auth

[機能]

自動鍵交換用 IPsec 情報の認証情報の設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike auth <auth_algo>[,<auth_algo>...]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<auth_algo>

認証アルゴリズムを指定します。
複数のアルゴリズムを指定することができます。複数定義するときは、アルゴリズムを空白なしでカンマ','で区切ります。

- hmac-md5
- hmac-sha1
- none

[説明]

送受信パケットを認証するための、認証アルゴリズムと鍵の設定を行います。
認証鍵は自動生成されるので、設定は不要です。
認証アルゴリズムを複数指定する場合、指定順序にかかわらず以下の優先順位となります。

1) hmac-md5
2) hmac-sha1

[未設定時]

IPsec によるパケット認証は行われません。

```
remote <number> ap <ap_number> ipsec ike auth none
```

5.2.37 remote ap ipsec ike pfs

[機能]

自動鍵交換用 IPsec 情報の PFS グループの設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike pfs <pfs_group>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<pfs_group>

Diffie-Hellman グループについて指定します。

- modp768
  Diffie-Hellman グループの MODP768
- modp1024
  Diffie-Hellman グループの MODP1024
- off
  Diffie-Hellman グループを使用しません。

[説明]

IPsec セッションの鍵素材を保護する、PFS グループの設定を行います。

[未設定時]

PFS による鍵交換データ保護は行いません。セキュア通信を行いたい場合は適切な PFS グループを設定してください。

```
remote <number> ap <ap_number> ipsec ike pfs off
```

5.2.38　remote ap ipsec ike lifetime

[機能]

自動鍵交換用 IPsec 情報の SA 有効時間の設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike lifetime <lifetime>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<lifetime>

- SA 有効時間
  SA 有効時間を、600 秒 (10 分)～86400 秒 (1 日) の範囲で指定します。単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。

[説明]

IPsec セッションの通信データを保護する、IPsec SA の SA 有効時間 (秒) の設定を行います。

[未設定時]

IPsec SA の有効時間として 8h(8 時間) が設定されたものとして扱います。

```
remote <number> ap <ap_number> ipsec ike lifetime 8h
```

5.2.39 remote ap ipsec ike newsa initiator

[機能]

自動鍵交換用 IPsec 情報の New SA Initiator(更新時間) の設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike newsa initiator <time>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time>

- Initiator SA 更新時間
  Initiator SA 更新時間を、30 秒～180 秒 (3 分) の範囲で指定します。単位は、m(分)、s(秒) のいずれかを指定します。

[説明]

自側が Initiator の場合に、IPsec SA の有効時間が満了になる前に、IPsec SA の更新を行うための時間の設定を行います。
相手側の New SA Responder と同じ時間にならないように設定してください。

[未設定時]

Initiator SA 更新時間として 90s(90 秒) が設定されたものとして扱います。

```
remote <number> ap <ap_number> ipsec ike newsa initiator 90s
```

5.2.40　remote ap ipsec ike newsa responder

[機能]

自動鍵交換用 IPsec 情報の New SA Responder(更新時間) の設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike newsa responder <time>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time>

- Responder SA 更新時間
  Responder SA 更新時間を、30 秒～180 秒 (3 分) の範囲で指定します。単位は、m(分)、s(秒) のいずれかを指定します。
- off
  Responder 側からの SA 更新は行いません。

[説明]

自側が Responder の場合に、IPsec SA の有効時間が満了になる前に、IPsec SA の更新を行うための時間の設定を行います。
相手側の New SA Initiator と同じ時間にならないように設定してください。
また、off 指定時には Responder 側からの SA 更新は行いません。

[未設定時]

Responder SA 更新時間として 30s(30 秒) が設定されたものとして扱います。

```
remote <number> ap <ap_number> ipsec ike newsa responder 30s
```

5.2.41 remote ap ipsec ike range

[機能]

自動鍵交換用 IPsec 情報の対象範囲の設定

[入力形式]

remote [<number>] ap [<ap_number>] ipsec ike range <src_addr>/<mask> <dst_addr>/<mask>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<src_addr>/<mask>

IPsec 対象となる送信元 IP アドレス、マスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  IPsec 対象となる送信元 IP アドレスとマスクビット数の組み合わせを指定します。
- any4
  すべての IPv4 アドレスを IPsec 対象に含めます。0.0.0.0/0(0.0.0.0/0.0.0.0) と同意。

<dst_addr>/<mask>

IPsec 対象となる宛先 IP アドレス、マスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  IPsec 対象となる宛先 IP アドレスとマスクビット数の組み合わせを指定します。
- any4
  すべての IPv4 アドレスを IPsec 対象に含めます。0.0.0.0/0(0.0.0.0/0.0.0.0) と同意。

[説明]

IPsec を適用するセッションの範囲を設定します。(Security Policy Database の情報)

[未設定時]

<src_addr>,<dst_addr>共に any4 が設定されたものとして扱います。

```
remote <number> ap <ap_number> ipsec ike range any4 any4
```

5.2.42　remote ap ike port

[機能]

IKE 情報の相手側 IKE ポート番号の設定

[入力形式]

remote [<number>] ap [<ap_number>] ike port <port>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<port>

- 相手側 IKE ポート番号
  相手側 IKE ポート番号を指定します。(デフォルト: 500 番)

[説明]

SA 確立のネゴシエーションを行う、相手 IKE サーバのポート番号の設定を行います。

[未設定時]

相手側 IKE ポート番号に標準ポート番号である 500 を指定したものとみなされます。

```
remote <number> ap <ap_number> ike port 500
```

5.2.43 remote ap ike shared key

[機能]

IKE セッション確立時の共通鍵 (Pre-shared key) の設定

[入力形式]

remote [<number>] ap [<ap_number>] ike shared key <kind> <shared_key>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<kind>

鍵種別を指定します。

- hex
  16 進数鍵を使用します。
- text
  文字列鍵を使用します。

<shared_key>

共通鍵を指定します。

- 暗号化されていない共通鍵を指定します。
  文字列鍵の場合は、0x22(ダブルクォーテーション) を除く [0x20-0x7e] の範囲のコードで構成される ASCII 文字列で指定します。ただし、文字列鍵で 0x20(空白文字) を使用する場合には、文字列鍵をダブルクォーテーション (") で囲う必要があります。以下に、入力範囲を示します。

鍵種別	16進数鍵	文字列鍵
共通鍵	1～256桁	1～128文字

- 暗号化された共通鍵を指定します。
  show コマンドで表示される暗号化された共通鍵を encrypted と共に指定します。show コマンドで表示される文字列をそのまま正確に指定してください。

<encrypted>

- 暗号化共通鍵指定
  <shared_key>に暗号化された共通鍵を指定する場合に指定します。

[説明]

SA 確立のネゴシエーションのときに接続相手を認証するための、共通鍵の設定を行います。

[未設定時]

共通鍵が設定されません。IKE により鍵交換を行う場合は必ず設定してください。

5.2.44　remote ap ike proposal delete

[機能]

IKE 情報の Proposal 定義の削除

[入力形式]

remote [<number>] ap [<ap_number>] ike proposal delete <proposal_number>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<proposal_number>

削除する Proposal 定義を指定します。

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。
- all
  <ap_number>で指定した IKE 情報のすべての Proposal 定義を削除対象とします。

[説明]

IKE 情報の Proposal 定義を削除します。

5.2.45 remote ap ike proposal move

[機能]

IKE セッション用 Proposal 定義優先順序の変更

[入力形式]

remote [<number>] ap [<ap_number>] ike proposal move <proposal_number> <new_number>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<proposal_number>

- 移動元の Proposal 定義優先順序を指定します。

<new_number>

- 移動先の Proposal 定義優先順序を指定します。

[説明]

<ap_number>で指定したアクセスポイント情報の IKE セッション用の Proposal 定義優先順序を変更します。
IKE セッション用 Proposal 定義とネゴシエーションの関係

	ネゴシエーション情報	Proposal	Proposal	...
a	暗号情報	3des-cbc	des-cbc	...
b	ハッシュ情報	hmac-md5	0	...
c	PFSグループ	modp768	modp1024	...
d	SA有効時間	600s	0	...

※ a を複数指定 (<proposal_number>0,1,2 を定義) した場合、ほかの情報は定義しなければ各情報のデフォルト値を採用します。
IKE セッションのネゴシエーションは、Proposal 単位 (a〜d を一組) として行います。その中で a〜c は相手装置の定義と一致することが条件となります。
自側が Responder の場合は、相手の Proposal が許容できるかを判断するため、自装置の定義は参照されません。
本装置を Aggressive Mode で動作させるときに、IKE セッション用 Proposal 定義を複数設定する場合、PFS の設定はすべて同じ値を設定してください。
これは、Aggressive Mode が Diffie-Hellman のグループについてネゴシエーションができないためです。(Initiator が最初の ISAKMP パケットに載せる鍵素材の計算に使用するため、Diffie-Hellman のグループは同じである必要があります) Aggressive Mode は、相手 (リモート) 情報 tunnel 利用時の自側の tunnel endpoint address を未設定にし、IKE 情報の自装置名を設定します。

5.2.46　remote ap ike proposal encrypt

[機能]

IKE セッション用暗号情報の設定

[入力形式]

remote [<number>] ap [<ap_number>] ike proposal [<proposal_number>] encrypt <enc_algo>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<proposal_number>

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。
  省略した場合は、0 を指定したものとみなされます。

<enc_algo>

暗号アルゴリズムを指定します。

- des-cbc
- 3des-cbc

[説明]

IKE セッションの送受信パケットを暗号化／復号化するための、暗号アルゴリズムの設定を行います。
コマンドによる定義を行う場合は、必ず設定してください。
IKE セッション用暗号情報設定が未定義だと IKE が動作しません。

[未設定時]

IKE セッション用暗号情報が設定されません。IKE により鍵交換を行う場合は必ず設定してください。

5.2.47 remote ap ike proposal hash

[機能]

IKE セッション用ハッシュ情報の設定

[入力形式]

remote [<number>] ap [<ap_number>] ike proposal [<proposal_number>] hash <hash_algo>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<proposal_number>

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。
  省略した場合は、0 を指定したものとみなされます。

<hash_algo>

ハッシュアルゴリズムを指定します。

- hmac-md5
- hmac-sha1

[説明]

IKE セッションのネゴシエーションパケットを認証するための、ハッシュアルゴリズムの設定を行います。

[未設定時]

ハッシュアルゴリズムに hmac-md5 を指定したものとみなされます。

```
remote <number> ap <ap_number> ike proposal <count> hash hmac-md5
```

5.2.48　remote ap ike proposal pfs

[機能]

IKE セッション用 PFS グループの設定

[入力形式]

remote [<number>] ap [<ap_number>] ike proposal [<proposal_number>] pfs <pfs_group>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<proposal_number>

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。
  省略した場合は、0 を指定したものとみなされます。

<pfs_group>

Diffie-Hellman グループについて指定します。

- modp768
  MODP768 の Diffie-Hellman グループ
- modp1024
  MODP1024 の Diffie-Hellman グループ

[説明]

IKE セッションのネゴシエーションパケットを保護するための、PFS グループの設定を行います。

[未設定時]

PFS グループに modp768 を指定したものとみなされます。

```
remote <number> ap <ap_number> ike proposal <count> pfs modp768
```

5.2.49 remote ap ike proposal lifetime

[機能]

IKE 情報の SA 有効時間の設定

[入力形式]

remote [<number>] ap [<ap_number>] ike proposal [<proposal_number>] lifetime <lifetime>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<proposal_number>

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。
  省略した場合は、0 を指定したものとみなされます。

<lifetime>

- SA 有効時間
  SA 有効時間を、600 秒 (10 分)～86400 秒 (1 日) の範囲で指定します。単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。

[説明]

IKE セッションのネゴシエーションパケットを保護するための、SA 有効時間 (秒) の設定を行います。

[未設定時]

IKE SA の有効時間として 24h(24 時間) が設定されたものとして扱われます。

```
remote <number> ap <ap_number> ike proposal <count> lifetime 24h
```

5.2.50　remote ap ike retry

[機能]

IKE 情報の初回再送時間および再送回数の設定

[入力形式]

remote [<number>] ap [<ap_number>] ike retry <time> <count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time>

- 初回再送時間初回再送時間を、1 秒～60 秒 (1 分) の範囲で指定します。単位は、m(分)、s(秒) のいずれかを指定します。

<count>

- 再送回数
  再送回数を、1～10 の範囲で指定します。

[説明]

IKE セッションのネゴシエーションパケットに対する初回再送時間および再送回数の設定を行います。

[未設定時]

初回再送時間に 10 秒、再送回数に 3 回を設定したものとみなされます。

```
remote <number> ap <ap_number> ike retry 10s 3
```

5.2.51 remote ap ike idtype

[機能]

IKE 情報の送信 ID タイプの設定

[入力形式]

remote [<number>] ap [<ap_number>] ike idtype <id_type>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<id_type>

ネゴシエーションの交換タイプを指定します。

- fqdn
  省略なしドメイン名
- user_fqdn
  省略なしユーザ識別名

[説明]

IKE セッションを確立する、ネゴシエーションの ID タイプの設定を行います。
IKE セッション確立のネゴシエーションパケットの ID payload に使用されます。

[未設定時]

IKE セッション確立のネゴシエーションパケットの ID タイプとして FQDN が設定されたものとして扱われます。

```
remote <number> ap <ap_number> ike idtype fqdn
```

5.2.52　remote ap ike name local

[機能]

IKE 情報の自装置名の設定

[入力形式]

remote [<number>] ap [<ap_number>] ike name local <name>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<name>

- 自装置名
  自装置を識別する名前を指定します。指定範囲は、1～64 文字です。
  名前は、0x22(ダブルクォーテーション) を除く [0x21-0x7e] の範囲のコードで構成される ASCII 文字列で指定します。ただし、"delete"を指定することはできません。

[説明]

IKE セッションを確立する、自装置の IP アドレスが不定の場合に名前の設定を行います。
IKE 情報の自装置名および相手装置名の設定と、相手 (リモート) 情報の tunnel endpoint address の設定により、ISAKMP SA のネゴシエーション交換タイプが以下のように決定します。

相手情報 IKE情報	tunnel local	tunnel remote
name local	動作しない	Aggressive Mode

tunnel local : tunnel 利用時の自側の tunnel endpoint address の設定
tunnel remote: tunnel 利用時の相手側の tunnel endpoint address の設定

[未設定時]

IKE セッション用自装置名が設定されません。Aggressive Mode により鍵交換を行う場合は必ず設定してください。

5.2.53 remote ap ike name local delete

[機能]

IKE 情報の自装置名の削除

[入力形式]

remote [<number>] ap [<ap_number>] ike name local delete

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

[説明]

IKE セッションを確立する自装置名の削除を行います。

5.2.54　remote ap ike release

[機能]

IPsec / IKE 情報の解放動作の設定

[入力形式]

remote [<number>] ap [<ap_number>] ike release <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

IPsec / IKE の SA 情報の解放動作設定を指定します。

- on
  回線切断時に解放処理を行います。
- off
  解放処理は行いません。

[説明]

自動鍵設定で作成された SA 情報の解放動作設定を行います。
on を指定した場合は、回線切断時に自動鍵設定が使用している SA 情報の解放動作を行います。
off を指定した場合は、回線切断時に自動鍵設定が使用している SA 情報の解放動作を行いません。

[注意]

本コマンドは、以下の回線切断動作時に有効です。

- ISDN(回線交換) を使用したときの回線切断時

[未設定時]

回線切断時に IKE SA 情報の解放を行うものとみなされます。

```
remote <number> ap <ap_number> ike release on
```

5.2.55 remote ap ike initial

[機能]

IKE ネゴシエーション開始動作の設定

[入力形式]

remote [<number>] ap [<ap_number>] ike initial <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

IKE ネゴシエーション開始動作を指定します。

- forward
  IPsec 対象パケットの送信を契機として、IPsec/IKE SA の確立動作を開始します。
- connect
  対象回線の接続または IPsec 対象パケットの送信を契機として、IPsec/IKE SA の確立動作を開始します。

[説明]

IKE ネゴシエーションを開始する契機を設定します。
<mode>に connect を指定した場合、回線接続または IPsec 対象パケットの送信を契機として、IKE ネゴシエーションを開始し、IPsec/IKE SA の確立を行います。

[注意]

本コマンドは、以下の回線接続時に有効です。

- ISDN(回線交換) を使用したとき

[未設定時]

IPsec 対象パケットの送信を契機として、IPsec/IKE SA の確立を行うものとみなされます。

```
remote <number> ap <ap_number> ike initial forward
```

5.2.56　remote ap ike sessionwatch

[機能]

IKE セッション監視の設定

[入力形式]

remote [<number>] ap [<ap_number>] ike sessionwatch <address> [<normal_interval> [<abnormal_interval>]]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<address>

- ICMP ECHO パケットの宛先 IP アドレス
  ICMP ECHO パケットの宛先 IP アドレスを指定します。
  IPsec 対象範囲に含まれる IP アドレスを指定してください。
  0.0.0.0 を指定した場合は、IKE セッションを監視しないものとみなされます。

<normal_interval>

- ICMP ECHO パケットの正常時送信間隔
  ICMP ECHO パケットの正常時送信間隔を、1 秒～60 秒 (1 分) の範囲で指定します。
  単位は、m(分)、s(秒) のいずれかを指定します。
  省略した場合は、10 秒を指定したものとみなされます。

<abnormal_interval>

- ICMP ECHO パケットの異常時送信間隔
  ICMP ECHO パケットの異常時送信間隔を、60 秒～600 秒 (10 分) の範囲で指定します。
  単位は、m(分)、s(秒) のいずれかを指定します。
  省略した場合は、180 秒 (3 分) を指定したものとみなされます。

[説明]

IKE セッションの生存確認を行うための動作情報を設定します。
指定した宛先 IP アドレスに対して ICMP ECHO パケットの送受信で生存確認を行います。
ICMP ECHO パケットの応答が正常に受信できている間は正常時送信間隔で監視を行いますが、ICMP ECHO パケットの応答が受信できなくなると、障害発生とみなし監視先に関連する IPsec / IKE SA を解放し、異常時送信間隔で監視を行います。
ICMP ECHO パケットの応答が受信できたときを復旧とみなし、監視先に関連する IPsec / IKE SA の確立を行い、正常送信間隔での監視に戻ります。

[未設定時]

IKE セッションの生存を監視しないものとみなされます。

```
remote <number> ap <ap_number> ike sessionwatch 0.0.0.0 10s 3m
```

5.2.57　remote ap tunnel local

[機能]

トンネル利用時の自側のトンネルエンドポイントアドレスの設定

[入力形式]

remote [<number>] ap [<ap_number>] tunnel local <address>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<address>

- 自側のトンネルエンドポイントアドレス
  自側のトンネルエンドポイントとなる IPv4 アドレスを指定します。本装置に設定されている IP アドレスを指定してください。
  0.0.0.0 を指定した場合は、設定を削除します。
  なお、IPv6 アドレスは指定できません。

[説明]

指定したアクセスポイント定義にトンネル利用が設定されている場合に、そのトンネルの自側エンドポイントアドレスを設定します。
トンネルを利用して通信を行う場合は、本コマンドを必ず実行してください。

[未設定時]

自側のトンネルエンドポイントアドレスを設定しないものとみなされます。

5.2.58 remote ap tunnel remote

[機能]

トンネル利用時の相手側のトンネルエンドポイントアドレスの設定

[入力形式]

remote [<number>] ap [<ap_number>] tunnel remote <address>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<address>

- 相手側のトンネルエンドポイントアドレス
  相手側のトンネルエンドポイントとなる IPv4 アドレスを指定します。
  0.0.0.0 を指定した場合は、設定を削除します。
  なお、IPv6 アドレスは指定できません。

[説明]

指定したアクセスポイント定義にトンネル利用が設定されている場合に、そのトンネルの相手側エンドポイントアドレスを設定します。
トンネルを利用して通信を行う場合は、本コマンドを必ず実行してください。

[未設定時]

相手側のトンネルエンドポイントアドレスを設定しないものとみなされます。

5.3　PPP 関連情報

5.3.1　remote ppp compress

[機能]

データ圧縮機能の設定

[入力形式]

remote [<number>] ppp compress <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

- off
  データ圧縮機能を使用しない場合に指定します。
- on
  データ圧縮機能を使用する場合に指定します。

[説明]

データ圧縮機能を使用するかどうか設定します。

[注意]

MP を使用する場合、受信順序制御 (“5.3.7 remote ppp mp order” を参照) を有効にしてください。MP を使用し、かつ受信順序制御を使用しないと定義している場合、ヒストリ機能 (高圧縮のための機能) を使用できません。

[未設定時]

データ圧縮機能を使用しないものとみなされます。

```
remote <number> ppp compress off
```

5.3.2 remote ppp mp start

[機能]

MP 利用時における初期接続リンク数の設定

[入力形式]

remote [<number>] ppp mp start <link>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<link>

- MP 利用時の初期接続リンク数
  MP 利用時の初期接続リンク数を指定します。

[説明]

MP 利用時の初期接続リンク数を設定します。
MP 利用時に自装置から発信する場合、最初から接続を試みるリンク数を設定します。なお、発信に失敗した場合、再試行は行いません。

[未設定時]

初期接続リンク数として 1 を指定したものとみなされます。

```
remote <number> ppp mp start 1
```

5.3.3　remote ppp mp resource analog

[機能]

アナログ発着信時の縮退動作の設定

[入力形式]

remote [<number>] ppp mp resource analog <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<mode>

- on
  アナログ発着信時に縮退動作を行います。
- off
  アナログ発着信時に縮退動作を行いません。

[説明]

MP 接続時に、アナログ発着信による縮退動作を行うかどうかを設定します。

[注意]

着信において縮退を行う場合には、「通信中着信通知」の契約が必要です。

[未設定時]

アナログ発着信時に縮退動作を行わないものとみなされます。

```
remote <number> ppp mp resource analog off
```

5.3.4 remote ppp mp traffic use

[機能]

自動チャネル数制御の可否の設定

[入力形式]

remote [<number>] ppp mp traffic use <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

- on
  スループット BOD の機能を使用します。
- off
  スループット BOD の機能を使用しません。

[説明]

スループット BOD 機能を使用するかどうかを設定します。

[未設定時]

スループット BOD 機能を使用しないとみなされます。

```
remote <number> ppp mp traffic use off
```

5.3.5　remote ppp mp traffic increase

[機能]

リンク増加閾値の設定

[入力形式]

remote [<number>] ppp mp traffic increase <traffic> <time>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<traffic>

- 回線増加閾値
  単位時間当たりにおけるチャネル利用率を、0〜100 の 10 進数値で指定します。
  以下に、回線増加閾値の計算式を示します。
  チャネル利用率 (%) = 転送バイト量 ÷ 転送可能バイト数 × 100

<time>

- 増加猶予時間
  トラフィックが回線増加閾値を超え続けた場合に、発信するまでの猶予時間を 0 秒〜3600 秒の範囲で指定します。単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。

[説明]

スループット BOD 機能使用時におけるリンク増加閾値を設定します。
スループット BOD 機能を使用する場合は、本コマンド を必ず設定してください。

[注意]

指定した増加猶予時間の間、チャネル利用率が回線増加閾値を超え続けた場合にチャネル増加のための発信が行われます。

[未設定時]

回線増加閾値および猶予時間を設定しないものとみなされます。

5.3.6 remote ppp mp traffic decrease

[機能]

リンク減少閾値の設定

[入力形式]

remote [<number>] ppp mp traffic decrease <traffic> <time>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<traffic>

- 回線減少閾値
  単位時間当たりにおけるチャネル利用率を、0～100 の 10 進数値で指定します。
  以下に、回線減少閾値の計算式を示します。
  チャネル利用率 (%) = 転送バイト量 ÷ 転送可能バイト数 × 100

<time>

- 減少猶予時間
  トラフィックが回線減少閾値を超え続けた場合に、切断するまでの猶予時間を 0 秒～3600 秒の範囲で指定します。単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。

[説明]

スループット BOD 利用時におけるリンク減少閾値を設定します。
スループット BOD 機能を使用する場合は、本コマンド を必ず設定してください。

[注意]

設定された減少猶予時間の間、チャネル利用率が回線減少閾値を下回り続けた場合にチャネル減少が行われます。

[未設定時]

回線減少閾値および猶予時間を設定しないものとみなされます。

5.3.7　remote ppp mp order

[機能]

受信パケット順序制御の有無の設定

[入力形式]

remote [<number>] ppp mp order <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

- off
  順序制御をしない場合に指定します。
- on
  順序制御をする場合に指定します。

[説明]

MP 受信パケットの順序制御を行うかどうか設定します。

[注意]

以下に、MP 受信パケットの順序制御が無効になっていると動作に影響が出る機能を示します。

- ブリッジ機能
  順序に依存するプロトコルをブリッジによって通信する場合、通信が停止することがあります。
- VJ ヘッダ圧縮機能
  設定にかかわらず、常に VJ ヘッダ圧縮を使用しません。
- IP ヘッダ圧縮機能
  設定にかかわらず、常に IP ヘッダ圧縮を使用しません。
- データ圧縮機能
  LZS アルゴリズムで、ヒストリ機能 (高効率圧縮の機能) を使用しません。

[未設定時]

MP 受信パケットの順序制御をしないものとみなされます。

```
remote <number> ppp mp order off
```

5.3.8 remote ppp ipcp vjcomp

[機能]

VJ-Compression の利用の有無の設定

[入力形式]

remote [<number>] ppp ipcp vjcomp <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

- enable
  VJ ヘッダ圧縮を使用する場合に指定します。
- disable
  VJ ヘッダ圧縮を使用しない場合に指定します。

[説明]

VJ ヘッダ圧縮機能 (VJCOMP) を使用するかどうかを設定します。VJ ヘッダ圧縮機能は、RFC1144 に準拠しています。

[注意]

MP を使用する場合は、“5.3.7 remote ppp mp order” の<mode>に on を指定して、受信順序制御を使用してください。
MP を使用するにもかかわらず受信順序制御を使用しないと定義している場合、VJ ヘッダ圧縮機能は無条件に無効となります。

[未設定時]

VJ ヘッダ圧縮機能を使用するものとみなされます。

```
remote <number> ppp ipcp vjcomp enable
```

5.3.9　remote ppp ipcp iphc

[機能]

IPv4 における IP ヘッダ圧縮 (IPHC) の設定

[入力形式]

remote [<number>] ppp ipcp iphc <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

- enable
  IP ヘッダ圧縮を使用する場合に指定します。
- disable
  IP ヘッダ圧縮を使用しない場合に指定します。

[説明]

IPv4 において、IP ヘッダ圧縮 (IPHC) を使用するかどうかを設定します。IP ヘッダ圧縮機能は、圧縮方法が RFC2507 / RFC2508 に、ネゴシエーション方法が RFC2509 に準拠しています。

[注意]

MP を使用する場合は、“5.3.7 remote ppp mp order” の<mode>に on を指定して、受信順序制御を使用してください。
MP を使用するにもかかわらず受信順序制御を使用しないと定義している場合、IP ヘッダ圧縮機能は無条件に無効となります。

[未設定時]

IP ヘッダ圧縮機能を使用しないものとみなされます。

```
remote <number> ppp ipcp iphc disable
```

5.3.10 remote ppp ipv6cp iphc

[機能]

IPv6 における IP ヘッダ圧縮 (IPHC) の設定

[入力形式]

remote [<number>] ppp ipv6cp iphc <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

- enable
  IP ヘッダ圧縮を使用する場合に指定します。
- disable
  IP ヘッダ圧縮を使用しない場合に指定します。

[説明]

IPv6 において、IP ヘッダ圧縮 (IPHC) の使用するかどうかを設定します。
IP ヘッダ圧縮機能は、圧縮方法が RFC2507 / RFC2508 に、ネゴシエーション方法が RFC2509 に準拠しています。

[注意]

MP を使用する場合は、“5.3.7 remote ppp mp order” の<mode>に on を指定して、受信順序制御を使用してください。
MP を使用するにもかかわらず受信順序制御を使用しないと定義している場合、IP ヘッダ圧縮機能は無条件に無効となります。

[未設定時]

IPv6 ヘッダ圧縮機能を使用しないものとみなされます。

```
remote <number> ppp ipv6cp iphc disable
```

5.4　IP 関連情報

5.4.1　remote ip address local

[機能]

自側 IP アドレスの設定

[入力形式]

remote [<number>] ip address local <address>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<address>

- 自側 IP アドレス
  相手ネットワークでの自側 IP アドレスを指定します。
  0.0.0.0 を指定した場合は、設定を削除します。

[説明]

相手ネットワークでの自側 IP アドレスを設定します。

[未設定時]

IP アドレスなし (unnumbered) として動作します。

5.4.2 remote ip address remote

[機能]

相手側 IP アドレスの設定

[入力形式]

remote [<number>] ip address remote <address>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<address>

- 相手側 IP アドレス
  相手ネットワークでの相手側 IP アドレスを指定します。
  0.0.0.0 を指定した場合は、設定を削除します。

[説明]

相手ネットワークでの相手側 IP アドレスを設定します。

[未設定時]

相手装置のアドレスが任意のアドレスであるものとして扱います。相手装置にアドレスがない場合、IP アドレスを割り当てません。

5.4.3　remote ip route add

[機能]

IPv4 スタティックルーティング情報 (静的経路情報) の設定

[入力形式]

remote [<number>] ip route add <address> / <mask> [<metric> [<distance>]]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<address>/<mask>

- IPv4 アドレス / マスクビット数 (またはマスク値)
  宛先ネットワークを IPv4 アドレスとマスクビット数の組み合わせで指定します。
  マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。
  - IPv4 アドレス / マスクビット数 (例: 192.168.1.0 / 24)
  - IPv4 アドレス / マスク値 (例: 192.168.1.0 / 255.255.255.0)
- default
  宛先ネットワークとしてデフォルトルートを設定する場合に指定します。
  0.0.0.0 / 0(0.0.0.0 / 0.0.0.0) を指定するのと同じ意味になります。

<metric>

- RIP メトリック値
  このスタティックルーティング情報を RIP で広報する場合のメトリック値を、1〜15 の 10 進数値で指定します。
  省略した場合は、1 を指定したものとみなされます。RIP 広報メトリック値は、以下の計算式で決定されます。
  - RIP 広報メトリック値=出力インタフェースの設定メトリック値+1+<metric>

<distance>

- 優先度
  このスタティックルーティング情報の優先度を、0〜254 の 10 進数値で指定します。優先度は値が小さい方が高い優先度を示します。
  省略した場合は、0 を指定したものとみなされます。

[説明]

相手ネットワークに対して、IPv4 スタティックルーティング (静的経路) を設定します。<distance>で設定した優先度は、IPv4 ルーティングプロトコルで受信した経路の優先度と比較され同じ経路の場合は優先度の高い方が選択されます。
IPv4 スタティックルーティング情報は、本装置全体で 64 個まで定義できます。

[注意]

<address> / <mask>がまったく同じ宛先に対し、1 つのスタティックルーティング情報が設定できます。

[未設定時]

IPv4 スタティックルーティング情報を設定しないものとみなされます。

5.4.4 remote ip route modify

[機能]

IPv4 スタティックルーティング情報 (静的経路情報) の修正

[入力形式]

remote [<number>] ip route modify <old_address>/<old_mask> <new_address>/<new_mask> [<new_metric> [<new_distance>]]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<old_address>/<old_mask>

- IPv4 アドレス/マスクビット数 (またはマスク値)
  修正前の宛先ネットワークを IPv4 アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。
  以下に、有効な記述形式を示します。
  - IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
  - IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)
- default
  修正前の宛先ネットワークにデフォルトルートを設定している場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<new_address>/<new_mask>

- IPv4 アドレス/マスクビット数 (またはマスク値)
  新しい宛先ネットワークを IPv4 アドレスとマスクビット数の組み合わせで指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。
  - IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
  - IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)
- default
  新しい宛先ネットワークとしてデフォルトルートを設定する場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<new_metric>

- 新しいメトリック値
  新しいメトリック値を、1〜15 の 10 進数値で指定します。
  省略した場合は、1 を指定したものとみなされます。

<new_distance>

- 新しい優先度
  新しい優先度を、0〜254 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

[説明]

IPv4 スタティックルーティング情報を修正します。

5.4.5　remote ip route delete

[機能]

IPv4 スタティックルーティング情報 (静的経路情報) の削除

[入力形式]

remote [<number>] ip route delete <address> / <mask>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<address>/<mask>

- IPv4 アドレス / マスクビット数 (またはマスク値)
  削除する宛先ネットワークを IPv4 アドレスとマスクビット数の組み合わせで指定します。
- default
  デフォルトルートを削除する場合に指定します。
  0.0.0.0 / 0(0.0.0.0 / 0.0.0.0) を指定するのと同じ意味になります。
- all
  すべてのスタティックルーティングを削除する場合に指定します。

[説明]

IPv4 スタティックルーティング情報を削除します。

5.4.6 remote ip rip

[機能]

ダイナミックルーティング情報 (RIP) の設定

[入力形式]

remote [<number>] ip rip <send> <receive> <metric> [<ignore> [<password>]]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<send>

RIP の送信について指定します。

- v1
  RIPv1(Unicast または Broadcast) を送信します。自側 IP アドレスが設定されている場合は Unicast で送信します。設定されていない場合 (unnumbered) は Broadcast で送信します。
- v2
  RIPv2(Unicast または Broadcast) を送信します。自側 IP アドレスが設定されている場合は Unicast で送信します。設定されていない場合 (unnumbered) は Broadcast で送信します。
- v2m
  RIPv2(Multicast) を送信します。
- off
  RIP を送信しません。

<receive>

RIP の受信について指定します。

- v1
  RIPv1 を受信します。
- v2
  RIPv1, RIPv2 を受信します。
- off
  RIP を受信しません。

<metric>

- 加算メトリック値
  RIP 情報の加算メトリック値を、0〜16 の 10 進数値で指定します。
  RIP 広報メトリック値は、以下の計算式で決定されます。
  - RIP 広報メトリック値=RIP 受信パケットのメトリック値+1+<metric>

<ignore>

自装置に<password>を設定していないときに、パスワード付きの RIPv2 パケットを受信したときの破棄の動作を指定します。
省略した場合は、off を指定したものとみなされます。

- on
  受信した RIPv2 パケットを破棄します。
- off
  受信した RIPv2 パケットを破棄しません。

<password>

- RIPv2 パスワード
  <send>または<receive>に v2 を指定した場合のパスワードを、0x21,0x23～0x7e のコードで構成される 16 文字以内の ASCII 文字列で指定します。
  省略した場合は、パスワードなしとみなされます。

[説明]

相手ネットワークに、IPv4 ダイナミックルーティング情報 (RIP) を設定します。ダイナミックルーティングとはルータ間でルーティング情報をやりとりすることで、そのつど最適なルートを選択してデータ通信を行う方法です。

[注意]

ISDN またはフレームリレー (従量課金) の場合、RIP 情報を送信すると、思わぬ課金 (定期発信または長時間接続) が発生します。
"remote mtu"で MTU 値を 576 よりも小さい値に設定すると、RIPv1(Broadcast), RIPv2(Broadcast) のパケットを送信しない場合があります。MTU 値は 576 以上を設定してください。

[未設定時]

IPv4 ダイナミックルーティング (RIP) を使用しないものとみなされます。

```
remote <number> ip rip off off 0 off
```

5.4.7 remote ip nat mode

[機能]

アドレス変換の設定

[入力形式]

remote [<number>] ip nat mode <mode> [<address> <addr_number> [<time>]]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

アドレス変換 (NAT) を使用するかどうかを設定します。

- off
  NAT を使用しません。
- nat
  NAT を使用します。
- multi
  マルチ NAT を使用します。

<address>

- 先頭グローバル IP アドレス
  動的変換に使用するグローバル IP アドレスの先頭アドレスを指定します。
- any
  グローバル IP アドレスの先頭アドレスとして IPCP ネゴシエーションの結果を使用します。

<addr_number>

- グローバル IP アドレスの個数
  動的変換に使用するグローバル IP アドレスの個数を、1～16 の 10 進数値で指定します。

<time>

- 割り当て時間
  割り当てられた変換テーブルを解放するための無通信監視時間を、0 秒～86400 秒 (1 日) の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。0 秒を指定した場合は、変換テーブル解放のための監視を行いません。
  省略した場合は、5 分を指定したものとみなされます。

[説明]

相手ネットワークに対するアドレス変換 (NAT) の動作を設定します。

[未設定時]

アドレス変換は使用しないものとみなされます。

```
remote <number> ip nat mode off
```

5.4.8　remote ip nat static

[機能]

静的アドレス変換の設定

[入力形式]

remote [<number>] ip nat static <count> <private_addr> <private_port>
<global_addr> <global_port> [<protocol>]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 静的アドレス変換定義番号
  静的アドレス変換定義番号を、0〜63 の 10 進数値で指定します。

<private_addr>

- プライベート IP アドレス
  静的アドレス変換の対象となるプライベート側の IP アドレスを指定します。

<private_port>

- プライベートポート番号
  静的アドレス変換の対象となるプライベート側のポート番号を、1〜65535 の 10 進数値で指定します。
  グローバルポート番号に複数ポート番号を指定した場合には、変換後の複数ポートの先頭ポート番号を指定します。
- any すべてのプライベートポート番号に対して有効な設定となります。

<global_addr>

- グローバル IP アドレス
  静的アドレス変換の対象となるグローバル側の IP アドレスを指定します。
- any すべてのグローバル IP アドレスに対して有効な設定となります。

<global_port>

- グローバルポート番号
  静的アドレス変換の対象となるグローバル側のポート番号を、1〜65535 の 10 進数値で指定します。
  複数個のアドレスを設定する場合には 1000-1200 のようにハイフンで結んで指定します。なお、ポート番号の範囲指定は一組のみ指定可能です。
- any
  すべてのグローバルポート番号に対して有効な設定となります。

<protocol>

- プロトコル番号
  静的アドレス変換の対象となるプロトコル番号を指定します。
  省略した場合は、any を指定したものとみなされます。
- any
  すべてのプロトコル番号に対して有効な設定となります。

[説明]

相手ネットワークに対する静的アドレス変換を設定します。
静的アドレス変換の対象となるパケットは、プロトコル番号<protocol>のプライベート側の IP アドレス <private_addr> とポート番号 <private_port>、グローバル側の IP アドレス<global_addr>とポート番号 <global_port>の指定内容により交換されます。
静的アドレス変換は、本装置全体で 64 個まで定義できます。

[未設定時]

静的アドレス変換は設定されません。

5.4.9　remote ip nat static delete

[機能]

静的アドレス変換の削除

[入力形式]

remote [<number>] ip nat static delete <count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 静的アドレス変換定義番号
  静的アドレス変換定義番号を、0～63 の 10 進数値で指定します。
- all
  すべての静的アドレス変換定義番号を削除対象とします。

[説明]

指定した静的アドレス変換を削除します。

5.4.10 remote ip nat rule

[機能]

アドレス変換ルールの設定

[入力形式]

remote [<number>] ip nat rule <count> ftp <server_addr> [<server_start_port>]-[<server_end_port>] [<check>]
remote [<number>] ip nat rule <count> ftp <server_addr> <server_port> [<check>]
remote [<number>] ip nat rule <count> irc <server_addr> [<server_start_port>]-[<server_end_port>]
remote [<number>] ip nat rule <count> irc <server_addr> <server_port>
remote [<number>] ip nat rule <count> dns <server_addr> [<server_start_port>]-[<server_end_port>] [<check>]
remote [<number>] ip nat rule <count> dns <server_addr> <server_port> [<check>]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 変換ルール番号
  変換ルール番号を、0～31 の 10 進数値で指定します。

ftp, irc, dns

変換ルールの対象となるアプリケーションを指定します。

<server_addr>

- IP アドレス
  NAT に割り当てたグローバルアドレス以外のアドレスを指定します。ここで指定したアドレスを変換ルールの対象とします。
- any
  すべての IP アドレスを変換ルールの対象とします。
  any を指定した場合は、グローバル側とプライベート側の両方のアプリケーションサーバに対応します。
- global
  NAT に割り当てたグローバルアドレス以外のすべてのアドレスを変換ルールの対象とします。
  global を指定した場合には、グローバル側のアプリケーションサーバに対応します。
- local
  NAT に割り当てたグローバルアドレスを変換ルールの対象とします。local を指定した場合には、プライベート側のアプリケーションサーバに対応します。
- off
  指定したアプリケーションに対する変換ルールを無効にします。

<server_start_port>

アプリケーションサーバで待ち受けるポートの範囲指定の開始番号を示します。

<server_end_port>

アプリケーションサーバで待ち受けるポートの範囲指定の終了番号を示します。

<server_port>

アプリケーションサーバで待ち受けるポート番号を示します。

<check>

- on

  アプリケーションに ftp を指定した場合、ftp サーバのデータ転送用 IP アドレスおよびポート番号のチェックを行います。

  アプリケーションに dns を指定した場合、グローバル側にサーバが存在するときのみ有効となります。DNS の応答の UDP パケットのソース IP アドレスおよびソースポート番号が問い合わせの UDP パケットのディスティネーション IP アドレスおよびディスティネーションポート番号と同一かどうかチェックします。

  省略した場合は、on を指定したものとみなされます。

- off

  アプリケーションに ftp を指定した場合、ftp サーバのデータ転送用 IP アドレスおよびポート番号のチェックを行いません。

  アプリケーションに dns を指定した場合、IP アドレスおよびポート番号のチェックを行いません。

[説明]

相手ネットワークに対するアドレス変換ルールを設定します。
指定 IP アドレス、指定ポート番号で動作する指定アプリケーションに対応するサーバに対するアドレス変換の特殊対応の設定を行います。
アドレス変換ルールは、本装置全体で 32 個まで定義できます。

[未設定時]

アドレス変換ルールは設定されません。

5.4.11 remote ip nat rule delete

[機能]

アドレス変換ルールの削除

[入力形式]

remote [<number>] ip nat rule delete <count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 変換ルール番号
  削除する変換ルール番号を、0～31 の 10 進数値で指定します。
- all
  すべての変換ルールを削除対象とします。

[説明]

指定したアドレス変換ルールを削除します。

5.4.12　remote ip filter

[機能]

IP フィルタの設定

[入力形式]

remote [<number>] ip filter <count> <action> <src_addr>/<mask> <src_port> <dst_addr>/<mask> <dst_port> <protocol> <tcpconnect> [<tos>]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す番号を、0〜63 の 10 進数値で指定します。指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つフィルタリング定義がすでに存在する場合は、既存の定義を変更します。

<action>

フィルタリング対象に該当するパケットを透過するかどうかを設定します。

- pass
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。
- restrict
  該当するパケットを、回線が接続されていれば透過し、切断されていれば遮断します。

<src_addr>/<mask>

フィルタリング対象とする送信元 IP アドレスとマスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)
  フィルタリング対象とする送信元 IP アドレスとマスクビット数の組み合わせを指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。
  以下に、有効な記述形式を示します。
  - IP アドレス/マスクビット数 (例: 192.168.1.1/24)
  - IP アドレス/マスク値 (例: 192.168.1.1/255.255.255.0)
- any
  すべての送信元 IP アドレスをフィルタリング対象とする場合に指定します。0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<src_port>

フィルタリング対象とする送信元ポート番号を指定します。

- ポート番号

  フィルタリング対象とする送信元ポート番号を、1〜65535 の 10 進数値で指定します。複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。

  ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。

  以下に、有効な記述形式を示します。

  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)

- any

  すべての送信元ポート番号をフィルタリング対象とする場合に指定します。

<dst_addr>/<mask>

フィルタリング対象とする宛先 IP アドレスとマスクビット数を指定します。

- IP アドレス/マスクビット数 (またはマスク値)

  フィルタリング対象とする宛先 IP アドレスとマスクビット数の組み合わせを指定します。

  記述形式は、<src_addr>/<mask>と同様です。

- any

  すべての宛先 IP アドレスをフィルタリング対象とする場合に指定します。0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<dst_port>

フィルタリング対象とする宛先ポート番号を指定します。

- ポート番号

  フィルタリング対象とする宛先ポート番号を、1〜65535 の 10 進数値で指定します。

  記述形式は、<src_port>と同様です。

- any

  すべての宛先ポート番号をフィルタリング対象とする場合に指定します。

<protocol>

フィルタリング対象とするプロトコル番号を指定します。

- プロトコル番号

  フィルタリング対象とするプロトコル番号を、0〜255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。

  0 を指定した場合は、すべてのプロトコルをフィルタリング対象とします。

<tcpconnect>

- yes

  TCP プロトコルでコネクション接続要求をフィルタリング対象に含めます。

- no

  TCP プロトコルでコネクション接続要求をフィルタリング対象に含めません。

<tos>

フィルタリング対象とする TOS 値を指定します。
省略した場合は、any を指定したものとみなされます。

- TOS 値
  フィルタリング対象とする TOS 値を、0〜ff の 16 進数値で指定します。複数の TOS 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。
  TOS 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 00〜ff の 16 進数値 (例: ff = ff の TOS 値)
  - TOS 値-TOS 値 (例: 32-64 = 32 から 64 までの TOS 値)
  - TOS 値- (例: 80- = 80 から ff までの TOS 値)
  - -TOS 値 (例: -7f = 0 から 7f までの TOS 値)
  - TOS 値,TOS 値,… (例: 10,20,30- = 10 と 20 と 30 以降の TOS 値)
- any
  すべての TOS 値をフィルタリング対象とする場合に指定します。

[説明]

相手ネットワークに対する IP フィルタを設定します。
IP フィルタは、指定したアドレス、ポート番号、プロトコル、TOS 値と一致するパケットを透過または遮断します。設定した優先度順に一致するか調べ、一致した時点でフィルタリングされ、それ以降の設定は参照されません。
IP フィルタは、本装置全体で 64 個まで定義できます。

[未設定時]

IP フィルタを設定しないものとみなされ、すべてのパケットが透過します。

5.4.13 remote ip filter move

[機能]

IP フィルタの優先順序の変更

[入力形式]

remote [<number>] ip filter move <count> <new_count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義の番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、0～63 の 10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合には、その定義の前に挿入されます。

[説明]

IP フィルタの優先順序を変更します。

5.4.14　remote ip filter delete

[機能]

IP フィルタの削除

[入力形式]

remote [<number>] ip filter delete <count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

削除するフィルタリングを指定します。

- フィルタリング定義番号
  削除するフィルタリングの定義番号を指定します。
- all
  すべてのフィルタリングを削除する場合に指定します。

[説明]

IP フィルタを削除します。

5.4.15 remote ip tos

[機能]

TOS 値書き換え条件の設定

[入力形式]

remote [<number>] ip tos <count> <src_addr>/<mask> <src_port> <dst_addr>/<mask> <dst_port> <protocol> <tos> <new_tos>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- TOS 値書き換え定義番号
  TOS 値書き換え条件の優先度を表す定義番号を、0〜31 の 10 進数値で指定します。
  指定した値は、設定完了時に順方向にソートされてリナンバリングされます。また、指定した定義番号と同じ値を持つ TOS 値書き換え定義がすでに存在する場合は、既存定義の値を変更します。

<src_addr>/<mask>

- IP アドレス/マスクビット数 (またはマスク値)
  TOS 値書き換え対象となる送信元 IP アドレスとマスクビット数の組み合わせを指定します。マスク値は最上位ビットから 1 で連続した値にしてください。
  以下に、有効な記述形式を示します。
  - IP アドレス/マスクビット数 (例: 192.168.1.1/24)
  - IP アドレス/マスク値 (例: 192.168.1.1/255.255.255.0)
- any
  すべての送信元 IP アドレスを TOS 値書き換えの対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<src_port>

TOS 値書き換え対象となる送信元ポート番号を指定します。

- ポート番号
  TOS 値書き換え対象となる送信元ポート番号を、1〜65535 の 10 進数値で指定します。複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。
  ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)
- any
  すべてのポート番号を対象とする場合に指定します。

<dst_addr>/<mask>

TOS 値書き換え対象となる宛先 IP アドレス、マスクビット数を指定します。

- IP アドレス / マスクビット数 (またはマスク値)
  TOS 値書き換え対象となる宛先 IP アドレスとマスクビット数の組み合わせを指定します。
  記述形式は、<src_addr>/<mask>と同様です。
- any
  すべての宛先 IP アドレスを TOS 値書き換えの対象とする場合に指定します。0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<dst_port>

TOS 値書き換え対象となる宛先ポート番号を指定します。

- ポート番号
  TOS 値書き換え対象となる宛先ポート番号を、1〜65535 の 10 進数値で指定します。
  記述形式は、<src_port>と同様です。
- any
  すべてのポート番号を対象とする場合に指定します。

<protocol>

- プロトコル番号
  TOS 値書き換え対象となるプロトコル番号を、0〜255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。0 を指定した場合は、すべてのプロトコルを対象とします。

<tos>

- TOS 値
  書き換え対象となる TOS 値を、0〜ff の 16 進数値で指定します。複数の TOS 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。
  TOS 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 00〜ff の 16 進数値 (例: ff = ff の TOS 値)
  - TOS 値-TOS 値 (例: 32-64 = 32 から 64 までの TOS 値)
  - TOS 値- (例: 80- = 80 から ff までの TOS 値)
  - -TOS 値 (例: -7f = 0 から 7f までの TOS 値)
  - TOS 値,TOS 値,… (例: 10,20,30- = 10 と 20 と 30 以降の TOS 値)
- any
  すべての TOS 値を、TOS 値書き換えの対象とする場合に指定します。

<new_tos>

- TOS 値
  書き換える TOS 値を、0〜ff の 16 進数値で指定します。

[説明]

TOS 値書き換え条件を設定します。
条件に一致したパケットの TOS 値を、指定した TOS 値に書き換えます。TOS 値書き換え条件は、本装置全体で 32 個まで定義できます。

[未設定時]

TOS 値書き換えを行わないものとみなされます。

5.4.16 remote ip tos move

[機能]

TOS 値書き換え条件の優先度の変更

[入力形式]

remote [<number>] ip tos move <count> <new_count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 対象 TOS 値書き換え定義番号
  優先順序を変更する前の TOS 値書き換え定義番号を指定します。

<new_count>

- 移動先 TOS 値書き換え定義番号
  <count>に対する新しい順序を、0～31 の 10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合には、その定義の前に挿入されます。

[説明]

TOS 値書き換え条件の優先度を変更します。

5.4.17　remote ip tos delete

[機能]

TOS 値書き換え条件の削除

[入力形式]

remote [<number>] ip tos delete <count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- TOS 値書き換え定義番号
  削除する TOS 値書き換え定義番号を指定します。
- all
  すべての TOS 値書き換え定義を削除する場合に指定します。

[説明]

TOS 値書き換え条件を削除します。

5.4.18 remote ip priority

[機能]

帯域制御の設定

[入力形式]

remote [<number>] ip priority <count> <src_addr>/<mask> <src_port> <dst_addr>/<mask> <dst_port> <protocol> <tos> <width>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 帯域制御定義番号
  帯域制御定義番号を、0〜63 の 10 進数値で指定します。

<src_addr>/<mask>

帯域制御の対象となる送信元 IP アドレス、マスクビット数を指定します。

- 送信元 IP アドレス/マスクビット数 (またはマスク値)
  帯域制御の対象となる送信元 IP アドレスとマスクビット数の組み合わせを指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。
  以下に、有効な記述形式を示します。
  - IP アドレス/マスクビット数 (例: 192.168.1.1/24)
  - IP アドレス/マスク値 (例: 192.168.1.1/255.255.255.0)
- any
  すべての IP アドレスを帯域制御の対象とする場合に指定します。0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<src_port>

帯域制御の対象となる送信元ポート番号を指定します。

- ポート番号
  帯域制御の対象となる送信元ポート番号を、1〜65535 の 10 進数値で指定します。複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)
- any
  すべてのポート番号を対象とする場合に指定します。

<dst_addr>/<mask>

帯域制御の対象となる宛先 IP アドレス、マスクビット数を指定します。

- 宛先 IP アドレス/マスクビット数 (またはマスク値)
  帯域制御の対象となる宛先 IP アドレスとマスクビット数の組み合わせを指定します。
  記述形式は<src_addr>/<mask>と同様です。
- any
  すべての IP アドレスを帯域制御の対象とする場合に指定します。0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<dst_port>

帯域制御の対象となる宛先ポート番号を指定します。

- ポート番号
  帯域制御の対象となる宛先ポート番号を、1〜65535 の 10 進数値で指定します。
  記述形式は<src_port>と同様です。
- any
  すべてのポート番号を対象とする場合に指定します。

<protocol>

- プロトコル番号
  帯域制御の対象となるプロトコル番号を、0〜255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。
  0 を指定した場合は、すべてのプロトコルを対象とします。

<tos>

- TOS 値
  帯域制御の対象となる TOS 値を、0〜ff の 16 進数値で指定します。複数の TOS 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。
  TOS 値は、","(カンマ) および"-"(ハイフン) を使用して 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 00〜ff の 16 進数値 (例: ff = ff の TOS 値)
  - TOS 値-TOS 値 (例: 32-64 = 32 から 64 までの TOS 値)
  - TOS 値- (例: 80- = 80 から ff までの TOS 値)
  - -TOS 値 (例: -7f = 0 から 7f までの TOS 値)
  - TOS 値,TOS 値,… (例: 10,20,30- = 10 と 20 と 30 以降の TOS 値)
- any
  すべての TOS 値を、帯域制御の対象とする場合に指定します。

<width>

- 帯域
  0〜100 の 10 進数値で指定した場合、0 は非優先 (ベストエフォート)、100 は最優先、1〜99 は同じ相手ネットワーク中の定義となり、それぞれ指定した値の比で帯域を割り当てます。たとえば、同じ相手ネットワーク中の定義が 3 つあり、それぞれ<width>の値が 30、30、60 であった場合、帯域として 25%、25%、50%が割り当てられます。なお、1〜99 を指定した定義のそれぞれの合計値が 100 未満の場合、残った帯域は定義に一致しないデータ用の帯域となります。

[説明]

帯域制御を設定します。任意のプロトコル、アドレス、ポート、TOS 値を指定して、割り当てる帯域を指定します。
帯域制御は、本装置全体で 64 個まで定義できます。

[注意]

IPv4 以外のパケットは、すべて非優先 (ベストエフォート) として扱われます。

[未設定時]

帯域制御を行わないものとみなされます。

5.4.19　remote ip priority delete

[機能]

帯域制御の削除

[入力形式]

remote [<number>] ip priority delete <count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

削除する帯域制御を指定します。

- 削除する帯域制御定義番号
  削除する帯域制御定義番号を指定します。
- all
  すべての帯域制御を削除する場合に指定します。

[説明]

帯域制御を削除します。

5.4.20 remote ip msschange

[機能]

MSS 書き換えの設定

[入力形式]

remote [<number>] ip msschange <mss>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mss>

- MSS 値
  MSS の書き換え値を、0 または 160～1460 の 10 進数値で指定します。
  0 を指定した場合は、MSS を書き換えません。

[説明]

MSS 書き換え機能を利用する場合の、書き換え値を設定します。

[未設定時]

MSS 書き換え機能を利用しないものとみなされます。

```
remote <number> ip msschange 0
```

5.4.21　remote ip fragment sort

[機能]

フラグメント順序変更の設定

[入力形式]

remote [<number>] ip fragment sort <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

フラグメントされたパケットの順序が前後逆転して受信した場合に、順序変更をするかどうかを指定します。

- off
  順序変更しません。
- on
  順序変更します。

[説明]

本装置の NAT 機能では、フラグメントされたパケットの順序が前後逆転して受信した場合、そのパケットを破棄します。フラグメントされたパケットの順序が逆転しないように、あらかじめパケットを整列させる場合には、順序変更を行う設定にします。

[未設定時]

フラグメント順序変更をしないものとみなされます。

```
remote <number> ip fragment sort off
```

5.5 IPv6 関連情報

5.5.1 remote ip6 use

[機能]

IPv6 機能の設定

[入力形式]

remote [<number>] ip6 use <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

IPv6 パケットの送受信を行うかどうか指定します。

- on
  このインタフェースで、IPv6 パケットの送受信を行います。
- off
  このインタフェースで、IPv6 パケットの送受信を行いません。

[説明]

このインタフェースで、IPv6 機能を利用するかどうかを設定します。

[未設定時]

IPv6 機能を利用しないものとみなされます。

```
remote <number> ip6 use off
```

5.5.2　remote ip6 ifid

[機能]

IPv6 インタフェース ID の設定

[入力形式]

remote [<number>] ip6 ifid <interfaceID>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<interfaceID>

このインタフェースで利用する ID を指定します。

- auto
  本装置が持つ MAC アドレスから、EUI-64 形式の ID を自動生成する場合に指定します。
- インタフェース ID
  このインタフェースで利用する ID を、16 進数値で指定します。4 桁ずつ":"(コロン) で区切ってください。なお、各フィールドの先頭の 0 は省略できます (例: 2a0:c9ff:fe84:759)。

通常は auto を指定してください。特定のインタフェース ID を指定する場合は、同一の link 上でホストと衝突しない値を指定してください。

[説明]

このインタフェースで利用する、インタフェース ID を設定します。

[未設定時]

インタフェース ID を自動生成するものとみなされます。

```
remote <number> ip6 ifid auto
```

5.5.3 remote ip6 address

[機能]

IPv6 アドレスの設定

[入力形式]

remote [<number>] ip6 address <count> <address> / <prefixlen> <valid> <preferred> [<flags>]

[パラメタ]

<number>

- remote 定義番号
  remote 定義の通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- IPv6 アドレス定義番号
  IPv6 アドレスの定義番号を、0～3 の 10 進数値で指定します。

<address>

- IPv6 アドレス
  128-bit の IPv6 アドレスを指定します。

<prefixlen>

- プレフィックス長
  IPv6 アドレスに対するプレフィックス長として、64 を指定します。

<valid>

- valid lifetime の時間
  このインタフェースから RA(Router Advertisement メッセージ) を送信するときに、このプレフィックスに対する valid lifetime を、0 秒～365 日の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。
- infinity
  このインタフェースから RA を送信するときに、このプレフィックスに対する valid lifetime を無限とする場合に指定します。

<preferred>

- preferred lifetime の時間
  このインタフェースから RA を送信する場合に、このプレフィックスに対する preferred lifetime を、0 秒～365 日の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。<preferred>は、<valid>よりも短い時間となるように設定してください。<preferred>が<valid>よりも大きい場合、<valid>と同じ時間として扱われます。
- infinity
  このインタフェースから RA を送信する場合に、このプレフィックスに対する preferred lifetime を無限とします。

<flags>

- RA Prefix Information に付与されるフラグ
  このインタフェースから RA を送出する場合に、この prefix に対する flags フィールドの値を 16 進数値で設定します。
  省略した場合は、c0 を指定したものとみなされます。

[説明]

このインタフェースにおける IPv6 アドレスを設定します。<address>の指定において、<prefixlen>以降がすべて 0 の場合には、指定した値は IPv6 プレフィックスであると判断されます。この IPv6 プレフィックスとインタフェース ID によって、IPv6 アドレスが生成されます。

[未設定時]

Link local アドレス以外の IPv6 アドレスを設定しないものとみなされます。

5.5.4 remote ip6 address delete

[機能]

IPv6 アドレスの削除

[入力形式]

remote [<number>] ip6 address delete <count>

[パラメタ]

<number>

- remote 定義番号
  remote 定義の通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- IPv6 アドレス定義番号
  削除する IPv6 アドレスの定義番号を指定します。
- all
  すべての IPv6 アドレスを削除する場合に指定します。

[説明]

IPv6 アドレスを削除します。

5.5.5　remote ip6 ra mode

[機能]

Router Advertisement の動作の設定

[入力形式]

remote [<number>] ip6 ra mode <mode>

[パラメタ]

<number>

- remote 定義番号
  lan 定義の通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

- off
  RA の送信を行いません。
  定期送信、および host からの RS に対する RA の送信を行いません。
- send
  RA の送信を行います。
  定期送信、および host からの RS に対する RA の送信を行います。

[説明]

RA(Router Advertisement メッセージ) を送信するかどうかを設定します。

[未設定時]

RA の送信を行わないものとみなされます。

```
remote <number> ip6 ra mode off
```

5.5.6 remote ip6 ra interval

[機能]

Router Advertisement メッセージ送信間隔の設定

[入力形式]

remote [<number>] ip6 ra interval <max> <min> <lifetime>

[パラメタ]

<number>

- remote 定義番号
  remote 定義の通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<max>

- 最大送信間隔
  RA を定期送信する場合の最大送信間隔 (秒) を、4〜1800 の 10 進数値で設定します。

<min>

- 最小送信間隔
  RA を定期送信する場合の最小送信間隔 (秒) を、3〜<max>× 3/4 の 10 進数値で設定します。

<lifetime>

- Router Lifetime の値
  送信する RA の Router Lifetime の値を、0 または<max>〜9000 の 10 進数値で設定します。

[説明]

RA の送信間隔、および RA の Router Lifetime の値の設定を行います。RA は<min>〜<max>でランダムに決定された間隔で定期送信されます。

[未設定時]

最大送信間隔に 600 秒、最小送信間隔に 200 秒、Router Lifetime の値に 1800 が設定されたものとみなされます。

```
remote <number> ip6 ra interval 600 200 1800
```

5.5.7　remote ip6 ra mtu

[機能]

Router Advertisement メッセージに含める MTU option の設定

[入力形式]

remote [<number>] ip6 ra mtu <mtu>

[パラメタ]

<number>

- remote 定義番号
  remote 定義の通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mtu>

- MTU option の内容
  RA に含める MTU option の値を、0 または 1280～1500 の 10 進数値で設定します。
  0 を指定した場合は、RA に MTU option を含めません。

[説明]

RA に含める MTU option の値を設定します。

[未設定時]

送信する RA に MTU option を含めないものとみなされます。

```
remote <number> ip6 ra mtu 0
```

5.5.8 remote ip6 ra reachabletime

[機能]

Router Advertisement メッセージに含める Reachable Time の設定

[入力形式]

remote [<number>] ip6 ra reachabletime <time>

[パラメタ]

<number>

- remote 定義番号
  remote 定義の通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time>

- Reachable Time の値
  RA に含める Reachable Time の値を、0～3600000 の 10 進数値で設定します。

[説明]

RA に含める Reachable Time の値を設定します。

[未設定時]

Reachable Time の値として 0 が設定されたものとみなされます。

```
remote <number> ip6 ra reachabletime 0
```

5.5.9　remote ip6 ra retranstimer

[機能]

Router Advertisement メッセージに含める Retrans Timer の設定

[入力形式]

remote [<number>] ip6 ra retranstimer <time>

[パラメタ]

<number>

- remote 定義番号
  remote 定義の通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time>

- Retrans Timer の値
  RA に含める Retrans Timer の値を、0～4294967295 の 10 進数値で設定します。

[説明]

RA に含める Retrans Timer の値を設定します。

[未設定時]

Retrans Timer の値として 0 が設定されたものとみなされます。

```
remote <number> ip6 ra retranstimer 0
```

5.5.10 remote ip6 ra curhoplimit

[機能]

Router Advertisement メッセージに含める Cur Hop Limit の設定

[入力形式]

remote [<number>] ip6 ra curhoplimit <CurHopLimit>

[パラメタ]

<number>

- remote 定義番号
  remote 定義の通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<CurHopLimit>

- Cur Hop Limit の値
  RA に含める Cur Hop Limit の値を、0〜255 の 10 進数値で設定します。

[説明]

RA に含める Cur Hop Limit の値を設定します。

[未設定時]

Cur Hop Limit の値として 64 が設定されたものとみなされます。

```
remote <number> ip6 ra curhoplimit 64
```

5.5.11　remote ip6 ra flags

[機能]

Router Advertisement メッセージに含める flags field の設定

[入力形式]

remote [<number>] ip6 ra flags <flags>

[パラメタ]

<number>

- remote 定義番号
  remote 定義の通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<flags>

- flags field の値
  RA に含める flags field の値を、00〜ff の 16 進数値で設定します。

[説明]

RA に含める flags field の値を設定します。

[未設定時]

flags field の値として 00 が設定されたものとみなされます。

```
remote <number> ip6 ra flags 00
```

5.5.12 remote ip6 route add

[機能]

IPv6 スタティックルーティング情報 (静的経路情報) の設定

[入力形式]

remote [<number>] ip6 route add <address>/<prefixlen> [<metric>]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<address>/<prefixlen>

- IPv6 アドレス/プレフィックス
  宛先ネットワークを IPv6 アドレスとプレフィックスの組み合わせを指定します。
- default
  宛先ネットワークとしてデフォルトルートを設定する場合に指定します。::/0 を指定するのと同じ意味になります。

<metric>

- メトリック値
  このスタティックルーティング情報を RIPng で広報する場合のメトリック値を、1〜15 の 10 進数値で指定します。
  省略した場合は、1 を指定したものとみなされます。
  RIPng 広報メトリック値は、以下の計算式で決定されます。
  - RIPng 広報メトリック値=出力インタフェースの設定メトリック値+1+<metric>

[説明]

IPv6 スタティックルーティング情報 (静的経路情報) を設定します。
IPv6 スタティックルーティング情報は、本装置全体で 64 個まで定義できます。

[未設定時]

IPv6 スタティックルーティング情報を設定しないものとみなされます。

5.5.13　remote ip6 route modify

[機能]

IPv6 スタティックルーティング情報 (静的経路情報) の修正

[入力形式]

remote [<number>] ip6 route modify <old_address>/<old_prefixlen>
<new_address>/<new_prefixlen> [<new_metric>]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<old_address>/<old_prefixlen>

修正前の IPv6 アドレスとプレフィックスの組み合わせを指定します。

- IPv6 アドレス/プレフィックス
  すでに定義されている宛先ネットワークの IPv6 アドレスとプレフィックスの組み合わせを指定します。
- default
  宛先ネットワークとしてデフォルトルートを登録する場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<new_address>/<new_prefixlen>

新しい IPv6 アドレスとプレフィックスの組み合わせを指定します。

- IPv6 アドレス/プレフィックス長
  新しい宛先ネットワークを IPv6 アドレスとプレフィックス長の組み合わせで指定します。
- default
  宛先ネットワークとしてデフォルトルートを登録する場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<new_metric>

- 新しいメトリック値
  新しいメトリック値を、1〜15 の 10 進数値で指定します。
  省略した場合は、1 を指定したものとみなされます。

[説明]

IPv6 スタティックルーティング情報 (静的経路情報) を修正します。

5.5.14 remote ip6 route delete

[機能]

IPv6 スタティックルーティング情報 (静的経路情報) の削除

[入力形式]

remote [<number>] ip6 route delete <address> / <prefixlen>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<address>/<prefixlen>

削除する IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長
  削除する IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- all
  すべてのスタティックルーティングを削除する場合に指定します。

[説明]

IPv6 スタティックルーティング情報 (静的経路情報) を削除します。

5.5.15　remote ip6 ripng

[機能]

ダイナミックルーティング情報 (RIPng) の設定

[入力形式]

remote [<number>] ip6 ripng <send> <receive> [<site> [<metric>]]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<send>

RIPng パケットを定期送信するかどうか指定します。

- on
  RIPng パケットを定期送信します。
- off
  RIPng パケットを定期送信しません。

<receive>

RIPng パケットを受信するかどうか指定します。

- on
  RIPng パケットを受信します。
- off
  RIPng パケットを受信しません。

<site>

site-local prefix を送受信するかどうか指定します。

- on
  site-local prefix を送受信します。
- off
  site-local prefix を送受信しません。

<send>および<receive>に off を指定した場合は、本パラメタにも off を指定してください。
省略した場合は、off を指定したものとみなされます。

<metric>

- 加算メトリック値
  RIPng 情報の加算メトリック値を、0〜16 の 10 進数値で指定します。<send>に off を指定した場合は省略できます。
  省略した場合は、0 を指定したものとみなされます。
  RIPng 広報メトリック値は、以下の計算式で決定されます。
  - RIPng 広報メトリック値=RIPng 受信パケットのメトリック値+1+<metric>

[説明]

IPv6 ダイナミックルーティングの動作を設定します。

[未設定時]

IPv6ダイナミックルーティング機能を使用しないものとみなされます。

```
remote <number> ip6 ripng off off off 0
```

5.5.16　remote ip6 aggregate

[機能]

ダイナミックルーティング情報 (RIPng) における経路集約の設定

[入力形式]

remote [<number>] ip6 aggregate <count> <address>/<prefixlen> <rejectroute>

[パラメタ]

<number>

- remote 定義番号
  remote 定義の通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 集約経路定義番号
  集約経路の定義番号を、0〜3 の 10 進数値で指定します。

<address>/<prefixlen>

- IPv6 アドレス/プレフィックス長
  集約経路の宛先ネットワークを IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- default
  集約経路としてデフォルトルートを登録する場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<rejectroute>

- on
  集約経路に対する破棄経路を設定します。
- off
  集約経路に対する破棄経路を設定しません。

[説明]

RIPng における集約経路の設定を行います。
集約経路が設定された場合には、設定された集約経路に含まれる個々の経路は広報されず、集約経路だけを広報します。また、集約経路と等しいネットワークに対する経路情報を持たない場合には、実際に持たない宛先に対するパケットを破棄するために、設定された集約経路に対する破棄経路を設定することもできます。
同一 remote 定義内に同一の集約経路は設定できません。

[未設定時]

経路集約は行わないものとみなされます。

5.5.17 remote ip6 aggregate delete

[機能]

ダイナミックルーティング情報 (RIPng) における経路集約の削除

[入力形式]

remote [<number>] ip6 aggregate delete <count>

[パラメタ]

<number>

- remote 定義番号
  remote 定義の通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 集約経路定義番号
  削除する集約経路の定義番号を、0～3 の 10 進数値で指定します。
- all
  すべての集約経路を削除する場合に指定します。

[説明]

集約経路の削除を行います。

5.5.18　remote ip6 filter

[機能]

IPv6 フィルタの設定

[入力形式]

remote [<number>] ip6 filter <count> <action> <src_addr> / <prefixlen> <src_port> <dst_addr> / <prefixlen> <dst_port> <protocol> <tcpconnect>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す番号を、0〜63 の 10 進数値で指定します。指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つフィルタリング定義がすでに存在する場合は、既存の定義を変更します。

<action>

フィルタリング対象に該当するパケットを透過するかどうかを設定します。

- pass
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。
- restrict
  該当するパケットを、回線が接続されていれば透過し、切断されていれば遮断します。

<src_addr>/<prefixlen>

フィルタリング対象とする送信元 IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス / プレフィックス長
  フィルタリング対象とする送信元 IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- any
  すべての送信元 IPv6 アドレスをフィルタリング対象とする場合に指定します。
  :: / 0 を指定するのと同じ意味になります。

<src_port>

フィルタリング対象とする送信元ポート番号を指定します。

- ポート番号
  フィルタリング対象とする送信元ポート番号を、1〜65535 の 10 進数値で指定します。複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。
  ポート番号は、","(カンマ) および"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。
  以下に、有効な記述形式を示します。

- 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
- ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
- ポート番号- (例: 1- = 1 から 65535 までのポート)
- -ポート番号 (例: -1000 = 1 から 1000 までのポート)
- ポート番号, ポート番号,… (例: 10,20,30- = 10 と 20 と 30 以降のポート)

- any
  すべての送信元ポート番号をフィルタリング対象とする場合に指定します。

<dst_addr>/<prefixlen>

フィルタリング対象とする宛先 IPv6 アドレスとプレフィックス長を指定します。

- IPv6 アドレス/プレフィックス長
  フィルタリング対象とする宛先 IPv6 アドレスとプレフィックス長の組み合わせを指定します。
- any
  すべての宛先 IPv6 アドレスをフィルタリング対象とする場合に指定します。
  ::/0 を指定するのと同じ意味になります。

<dst_port>

フィルタリング対象とする宛先ポート番号を指定します。

- ポート番号
  フィルタリング対象とする宛先ポート番号を、1〜65535 の 10 進数値で指定します。
  記述形式は、<src_port>と同様です。
- any
  すべての宛先ポート番号をフィルタリング対象とする場合に指定します。

<protocol>

フィルタリング対象とするプロトコル番号を指定します。

- プロトコル番号
  フィルタリング対象とするプロトコル番号を、0〜255 の 10 進数値で指定します。
  255 を指定した場合は、すべてのプロトコルをフィルタリング対象とします。

<tcpconnect>

- yes
  TCP プロトコルでコネクション接続要求をフィルタリング対象に含めます。
- no
  TCP プロトコルでコネクション接続要求をフィルタリング対象に含めません。

[説明]

相手ネットワークに対する IPv6 フィルタを設定します。各パラメタに設定された値によって、動作が変化する場合があります。以下に説明します。

- <protocol>に指定した値によって、IPv6 拡張ヘッダの扱いが以下のように変化します。
  - 255 を指定した場合は、0 個以上の IPv6 拡張ヘッダを含む、あらゆる upper-layer protocol(upper-layer protocol なしを含む) に一致します。
  - 以下の IPv6 拡張ヘッダの値を指定した場合は、その拡張ヘッダが付与されている、あらゆる upper-layer protocol(upper-layerprotocol なしを含む) のパケットが一致します。

    0 Hop-by-Hop Options Header

43　Routing Header

44　Fragment Header

60　Destination Options Header

- 以下の値を指定した場合は、0 個以上の IPv6 拡張ヘッダ (AH、ESP、IPComp を除く) を含む、upper-layer protocol ヘッダが付与されていないパケットが一致します。

  59　no next header

- その他の値が設定されている場合は、upper-layer protocol ヘッダの protocol 番号に等しい値であるパケットが一致します。この場合、AH、ESP、IPComp を除くすべての IPv6 拡張ヘッダは無視されます。パケット中に AH、ESP が設定されている場合は、それ以降の拡張ヘッダおよび upper-layer protocol ヘッダの解釈は行いません。

- <src_port>、<dst_port>に指定した値によって、<protocol>の扱いが以下のように変化します。
  - <protocol>に 255 を指定し、かつ<src_port>、<dst_port>のいずれか、または両方を指定している場合、TCP および UDP パケットの該当ポート番号を持つパケットのみが一致します。
  - <protocol>に TCP(6) または UDP(17) を指定し、かつ<src_port>、<dst_port>のいずれか、または両方を指定している場合、指定プロトコルの該当ポート番号を持つパケットのみが一致します。
  - <protocol>に TCP(6) または UDP(17) 以外を指定し、かつ<src_port>、<dst_port>のいずれか、または両方を指定している場合、あらゆるパケットが一致しません。

- <tcpconnect>の扱いを以下に示します。
  - <protocol>に any を指定した場合、TCP パケットのときにこの設定値が適用されます。
  - <protocol>に TCP(6) を指定した場合、常にこの設定値が適用されます。
  - <protocol>に any または TCP(6) 以外を指定した場合、この設定値は適用されません。

IPv6 フィルタは、本装置全体で 64 個まで定義できます。

[未設定時]

IPv6 フィルタを設定しないものとみなされ、すべてのパケットが透過します。

5.5.19 remote ip6 filter move

[機能]

IPv6 フィルタの優先順序の変更

[入力形式]

remote [<number>] ip6 filter move <count> <new_count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義の番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、0～63 の 10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合には、その定義の前に挿入されます。

[説明]

IPv6 フィルタの優先順序を変更します。

5.5.20　remote ip6 filter delete

[機能]

IPv6 フィルタの削除

[入力形式]

remote [<number>] ip6 filter delete <count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

削除するフィルタリングを指定します。

- フィルタリング定義番号
  削除するフィルタリングの定義番号を指定します。
- all
  すべてのフィルタリングを削除する場合に指定します。

[説明]

IPv6 フィルタを削除します。

5.6 ブリッジ関連情報

5.6.1 remote bridge use

[機能]

ブリッジ機能の設定

[入力形式]

remote [<number>] bridge use <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

ブリッジを使用するかどうかを指定します。

- on
  ブリッジを使用する場合に指定します。
- off
  ブリッジを使用しない場合に指定します。

[説明]

ブリッジを使用するかどうかを設定します。
ブリッジを使用する場合、IP および IPv6 のパケット以外をすべてブリッジします。
ただし、接続先との接続時に BCP のネゴシエーションを行い、ネゴシエーションが成功した場合にブリッジデータの送受信が可能となります。

[注意]

IP および IPv6 以外のネットワークプロトコル (IPX など) をルーティングしているネットワークでブリッジを使用する場合は、ブリッジによって中継されることでネットワークがダウンすることがあります。ルーティングと併用する場合は、ルーティングによって転送するプロトコルをフィルタリングするよう設定してください。

[未設定時]

ブリッジを使用しないものとみなされます。

```
remote <number> bridge use off
```

5.6.2　remote bridge stp use

[機能]

STP モードの設定

[入力形式]

remote [<number>] bridge stp use <mode>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

- on
  STP を使用する場合に指定します。
- off
  STP を使用しない場合に指定します。

[説明]

スパニングツリーアルゴリズムで経路制御を行うかどうかを設定します。
本コマンドは、ブリッジを使用している場合にだけ有効です。

[未設定時]

STP を使用しないものとみなされます。

```
remote <number> bridge stp use off
```

5.6.3 remote bridge stp cost

[機能]

パスコストの設定

[入力形式]

remote [<number>] bridge stp cost <path_cost>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<path_cost>

接続先と通信する場合のパスコストを指定します。

- auto
  インタフェースの速度に応じて、パスコストが自動決定されます。
  以下に、本パラメタ指定時のパスコストを示します。

回線種別	パスコスト
Ethernet(10Mbps)	100
HSD(64kbps)	15620
HSD(128kbps)	7810
FR(64kbps)	16000
FR(128kbps)	8500
ISDN(64kbps)	16000

- パスコスト
  パスコストを、1～65535 の 10 進数値で指定します。値が小さいほど、優先度が高くなります。

通常は auto を指定してください。ただし、ブリッジネットワークを構築するうえで、優先ブリッジ決定のために任意のパスコストを指定することができます。

[説明]

スパニングツリーアルゴリズムで使用するパスコストを設定します。
本コマンドは、STP を使用する場合にだけ有効です。

[未設定時]

パスコストを自動決定するとみなされます。

```
remote <number> bridge stp cost auto
```

5.6.4　remote bridge stp priority

[機能]

インタフェース優先度の設定

[入力形式]

remote [<number>] bridge stp priority <port_priority>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<port_priority>

- インタフェース優先度
  インタフェースごとの優先度を、0～255 の 10 進数値で指定します。値が小さいほど、優先度が高くなります。

[説明]

スパニングツリーアルゴリズムで使用する、インタフェースごとの優先度を設定します。通常、設定する必要はありません。
本コマンドは、STP を使用する場合にだけ有効です。
本コマンドを設定しない場合は、<number>で指定したインタフェースが優先となり、remote 定義で定義されたインタフェースが非優先となります。lan 定義内で定義されたインタフェースでは、定義番号のもっとも小さいものが優先されます。

[未設定時]

インタフェース優先度に 128 が設定されたものとみなされます。

```
remote <number> bridge stp priority 128
```

5.6.5 remote bridge filter

[機能]

MAC フィルタの設定

[入力形式]

remote [<number>] bridge filter <count> <action> <src_mac> <dst_mac> <format> <value>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す番号を、0〜127 の 10 進数値で指定します。指定した値は、設定完了時に順方向にソートされリナンバリングされます。
  指定した定義番号と同じ値を持つ定義がすでに存在する場合は、既存の設定に対する修正とみなされます。指定した値を持つ定義が存在しない場合は、追加とみなされます。

<action>

フィルタリング対象に該当するパケットを透過するかどうかを指定します。

- pass
  該当するパケットを透過します。
- reject
  該当するパケットを遮断します。
- restrict
  該当するパケットを、回線が接続されていれば透過し、切断されていれば遮断します。

<src_mac>

フィルタリング対象とする送信元 MAC アドレスを指定します。

- any
  すべての MAC アドレスを対象とする場合に指定します。
- bcast
  ブロードキャスト MAC アドレスを対象とする場合に指定します。
- mcast
  マルチキャスト MAC アドレスを対象とする場合に指定します。
- 上記以外
  対象とする MAC アドレスを指定します。フィルタリング対象とする送信元 MAC アドレスを、xx:xx:xx:xx:xx:xx(xx は 2 桁の 16 進数値) の形式で指定します。

<dec_mac>

フィルタリング対象とする宛先 MAC アドレスを指定します。

- any
  すべての MAC アドレスを対象とする場合に指定します。
- bcast
  ブロードキャスト MAC アドレスを対象とする場合に指定します。
- mcast
  マルチキャスト MAC アドレスを対象とする場合に指定します。
- 上記以外
  対象とする MAC アドレスを指定します。フィルタリング対象とする送信元 MAC アドレスを、xx:xx:xx:xx:xx:xx(xx は 2 桁の 16 進数値) の形式で指定します。

<format> <value>

- llc
  <value>の値と LSAP が一致する LLC 形式パケットを対象とする場合に指定します。<value>には、0～ffff の 16 進数値を指定します。
- ether
  <value>の値とタイプが一致する Ethernet 形式パケットを対象とする場合に指定します。<value>には、5dd～ffff の 16 進数値を指定します。
- any
  すべてのパケットを対象とする場合に指定します。<value>は、指定不要です。

[説明]

MAC フィルタを設定します。
本コマンドは、ブリッジ機能を使用する場合にだけ有効です。
指定した条件に一致するパケットを、指定した<action>に従って遮断または通過させます。
MAC フィルタは、本装置全体で 128 個まで定義できます。

[注意]

IP および IPv6 以外のネットワークプロトコル (IPX など) をルーティングしているネットワークでブリッジを使用する場合は、ブリッジによって中継されることでネットワークがダウンすることがあります。ルーティングと併用する場合は、ルーティングによって転送するプロトコルをフィルタリングするよう設定してください。

[未設定時]

MAC フィルタを設定しないものとみなされ、すべてのパケットが透過します。

5.6.6 remote bridge filter move

[機能]

MAC フィルタの優先順序の変更

[入力形式]

remote [<number>] bridge filter move <count> <new_count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 対象フィルタリング定義番号
  優先順序を変更する前のフィルタリング定義の番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、0～127 の 10 進数値で指定します。
  すでにこの定義番号を持つ定義が存在する場合には、その定義の前に挿入されます。

[説明]

MAC フィルタの優先順序を変更します。

5.6.7　remote bridge filter delete

[機能]

MAC フィルタ情報の削除

[入力形式]

remote [<number>] bridge filter delete <count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- フィルタリング定義番号
  削除するフィルタリングの定義番号を指定します。
- all
  すべてのフィルタリング情報を削除する場合に指定します。

[説明]

MAC フィルタ情報を削除します。

5.7　マルチホーミング関連情報

5.7.1　remote multihoming mode

[機能]

マルチホーミング機能の設定

[入力形式]

remote [<number>] multihoming mode <mode> [<judge>]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

マルチホーミングのセッション切り分け方式を指定します。

- off
  マルチホーミング機能を使用しません。
- onebyone
  順次方式を使用します。
- roundrobin
  ラウンドロビン方式を使用します。
- both
  双方方式を使用します。

<judge>

<mode>が onebyone(順次方式) または both(双方方式) の場合にだけ有効であり、それ以外の場合に<judge>があればエラーとなります。

- session
  セッション数を閾値として使用します。
- rate
  WAN の回線使用率を閾値として使用します。
- speed
  WAN の回線使用速度を閾値として使用します。

[説明]

マルチホーミング機能 (負荷分散・高信頼性機能) を使用する場合のセッションの切分け方式を設定します。"onebyone"、"roundrobin"、"both"の場合はマルチホーミング機能を使用します。"off"の場合は使用しません。

- onebyone (順次方式)
  順次方式ではセッション数または WAN 側経路使用率が設定値を超えるまでは新しいセッションを WAN 側セッションとし、設定値を超えてからは転送セッションとします。
  切分けの閾値は"remote multihoming session"と"remote multihoming rate"と"remote multihoming speed"コマンドにより設定します。

- roundrobin (ラウンドロビン方式)
  ラウンドロビン方式では WAN 側セッションと転送セッションの比率が指定した割合になるようにセッションを切り分けます。
  セッション数の割合は"remote multihoming ratio"コマンドにより設定します。
- both (双方方式)
  双方方式では閾値 (セッション数または回線使用率) を超えるまでは順次方式、閾値を超えてからはラウンドロビン方式を使用します。
  切分けの閾値は"remote multihoming session"と"remote multihoming rate"と"remote multihoming speed"コマンドにより設定します。

[未設定時]

マルチホーミング機能を使用しないものとみなされます。

```
remote <number> multihoming off
```

5.7.2 remote multihoming session

[機能]

最大セッション数の設定

[入力形式]

remote [<number>] multihoming session <value>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<value>

- 最大セッション数
  最大セッション数を、0～256 の範囲で指定します。

[説明]

順次方式と双方方式で閾値として使用するセッション数を指定します。

[未設定時]

最大セッション数として、0 を設定したものとみなされます。

```
remote <number> multihoming session 0
```

5.7.3　remote multihoming rate

[機能]

最大回線使用率の設定

[入力形式]

remote [<number>] multihoming rate <value>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<value>

- 最大回線使用率
  最大回線使用率 [%] を、0〜100 の範囲で指定します。

[説明]

順次方式と双方方式で閾値として使用する回線使用率を指定します。

[未設定時]

最大回線使用率として、0[%] を設定したものとみなされます。

```
remote <number> multihoming rate 0
```

5.7.4 remote multihoming speed

[機能]

最大回線使用速度の設定

[入力形式]

remote [<number>] multihoming speed <value>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<value>

- 最大回線使用速度
  最大回線使用速度を、0k～128K の範囲の 10 進数値と単位文字で指定します。
  10 進数値の末尾に k の単位文字を付与することで単位を指定できます。
  単位文字を付与しない場合、単位は Kbps となります。
  単位文字 k を付与した場合、単位は Kbps となります。
  1Kbps は 1000bps です。

[説明]

順次方式と双方方式で閾値として使用する回線使用速度を指定します。

[未設定時]

最大回線使用速度として、0 Kbps を設定したものとみなされます。

```
remote <number> multihoming speed 0k
```

5.7.5　remote multihoming ratio

[機能]

WAN 側セッションと転送側セッションの比率の設定

[入力形式]

remote [<number>] multihoming ratio <ratio>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<ratio>

- WAN 側セッションの割合
  WAN 側セッションの割合を、0～10 の範囲で指定します。

[説明]

ラウンドロビン方式で使用します。WAN 側セッションの割合を設定します。
<ratio>を x と設定した場合、2 つのセッションの比率は以下のようになります。

- WAN 側セッション数 : 転送セッション数 = x : (10 - x)

[未設定時]

WAN 側セッションの割合として、0 を設定したものとみなされます。

```
remote <number> multihoming ratio 0
```

5.7.6 remote multihoming timeout

[機能]

セッションタイムアウト時間の設定

[入力形式]

remote [<number>] multihoming timeout <time>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time>

- セッションタイムアウト時間
  セッションタイムアウト時間を、60 秒 (1 分)～86400 秒 (1 日) の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。

[説明]

動的マルチホーミング情報テーブルのセッション情報がタイムアウトとなり削除される時間を設定します。テーブルに記録されているセッションについて無通信状態が設定された時間継続した場合に該当セッション情報をテーブルから削除します。

[未設定時]

セッションタイムアウト時間として、5 分を設定したものとみなされます。

```
remote <number> multihoming timeout 5m
```

5.7.7　remote multihoming router

[機能]

転送先ルータ IP アドレスの設定

[入力形式]

remote [<number>] multihoming router <address>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<address>

- 転送先ルータ IP アドレス
  転送先ルータ IP アドレスを指定します。
  0.0.0.0 を指定した場合、転送セッション (LAN 側の転送先ルータ経由のセッション) となったパケットは破棄されます。

[説明]

転送先ルータの IP アドレスを設定します。
転送セッションのパケットは本装置からこの IP アドレスを持つ転送先ルータに転送されます。

[未設定時]

転送先ルータの IP アドレスとして、0.0.0.0 を設定したものとみなされます。

```
remote <number> multihoming router 0.0.0.0
```

5.7.8 remote multihoming watchdog address

[機能]

転送セッション経路監視用 IP アドレスの設定

[入力形式]

remote [<number>] multihoming watchdog address <address>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<address>

- 転送セッション経路監視用 IP アドレス
  転送セッション経路監視用 IP アドレスを指定します。
  0.0.0.0 を指定した場合は、監視しません。

[説明]

転送セッションの経路状態を監視するための ping(ICMP Echo) の宛先 IP アドレスを設定します。
この IP アドレスに対して転送先ルータ経由で指定した間隔で ping を実行し、WAN 経路の状態を監視します。
ping を実行する間隔は、"multihoming watchdog interval"で設定します。

[未設定時]

転送セッション経路を監視しないものとみなされます。

```
remote <number> multihoming watchdog address 0.0.0.0
```

5.7.9　remote multihoming watchdog interval

[機能]

転送セッション経路監視用の ping 実行間隔の設定

[入力形式]

remote [<number>] multihoming watchdog interval <time>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time>

- 転送セッション経路監用 ping 実行間隔
  転送セッション経路を監視するための ping(ICMP Echo) 実行間隔を、1 秒～255 秒の範囲で指定します。
  単位は、m(分)、s(秒) のいずれかを指定します。

[説明]

転送セッション経路監視のための ping の実行間隔を設定します。

[未設定時]

転送セッション経路監視用 ICMP Echo (ping) の送信間隔として 10 秒を設定したものとみなされます。

```
remote <number> multihoming watchdog interval 10s
```

5.7.10 remote multihoming watchdog response

[機能]

障害認識無応答回数と障害復旧判断応答回数の設定

[入力形式]

remote [<number>] multihoming watchdog response <error> <recovery>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<error>

- 障害認識無応答回数
  ICMP Echo Reply を連続して受信しなかった場合に障害を認識する回数を、1～16 の範囲の 10 進数で指定します。

<recovery>

- 障害復旧判断応答回数
  ICMP Echo Reply を連続して受信した場合に障害からの復旧を認識する回数を、1～16 の範囲の 10 進数で指定します。

[説明]

転送セッション経路監視用 ping の応答を<error>で設定した回数連続して受信できなかった場合に転送セッションの経路に障害が発生したと認識します。
転送セッションの経路に障害があると認識されている状態で、転送セッション経路監視用 ping の応答を<recovery>で設定した回数連続して受信した場合に障害から復旧したと認識します。

[未設定時]

障害認識無応答回数は 3 回、障害復旧判断応答回数は 1 回を設定したものとみなされます。

```
remote <number> multihoming watchdog response 3 1
```

5.7.11　remote multihoming static

[機能]

静的マルチホーミングの設定

[入力形式]

remote [<number>] multihoming static <count> <route> <change> <src_port> <dst_port> <protocol>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 静的マルチホーミング定義番号
  静的マルチホーミング情報の定義番号を、0〜63 の 10 進数値で指定します。
  指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つフィルタリング定義がすでに存在する場合は、既存の定義を変更します。

<route>

静的マルチホーミング対象のパケットを転送する経路を指定します。

- wan
  対象パケットを本装置の WAN 側に送出します。
- lan
  対象パケットを LAN 側の転送先ルータに転送します。

<change>

障害時に経路を変更するかどうかを指定します。

- enable <route>で指定した経路に障害が発生した場合に経路を変更します。・disable <route>で指定した経路に障害が発生した場合に対象パケットを破棄します。

<src_port>

静的マルチホーミング対象となる送信元ポート番号を指定します。

- 送信元ポート番号
  静的マルチホーミング対象となる送信元ポート番号を、1〜65535 の 10 進数値で指定します。複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。
  ポート番号は、","(カンマ) または"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号 … (例: 10,20,30- = 10 と 20 と 30 以降のポート)
- any
  すべてのポート番号を対象とする場合に指定します。

<dst_port>

静的マルチホーミング対象となる宛先ポート番号を指定します。

- 宛先ポート番号

  静的マルチホーミング対象となる宛先ポート番号を、1〜65535 の 10 進数値で指定します。複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。

  ポート番号は、","(カンマ) または"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。

  以下に、有効な記述形式を示します。

  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号 … (例: 10,20,30- = 10 と 20 と 30 以降のポート)

- any

  すべてのポート番号を対象とする場合に指定します。

<protocol>

- プロトコル番号

  静的マルチホーミング対象のプロトコル番号を、0〜255 の 10 進数値で指定します。(例: ICMP:1、TCP:6、UDP:17 など)。

  255 を指定すると、以下の any を指定したのと同じ意味になります。

- any

  すべてのプロトコル番号を対象とする場合に指定します。

[説明]

条件に一致するパケットは設定に従って WAN に送出されるか、または LAN 側の転送先ルータに転送されます。

[未設定時]

静的マルチホーミング情報を設定しないものとみなされます。

5.7.12　remote multihoming static move

[機能]

静的マルチホーミングの優先順序の変更

[入力形式]

remote [<number>] multihoming static move <count> <new_count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- 対象静的マルチホーミング定義番号
  優先順序を変更する静的マルチホーミング情報の定義番号を指定します。

<new_count>

- 移動先マルチホーミング定義番号
  <count>に対する新しい順序を、0～64 の 10 進数値で指定します。すでにこの番号を持つ定義が存在する場合には、その定義の前に挿入されます。

[説明]

静的マルチホーミング情報の優先順序を変更します。

5.7.13 remote multihoming static delete

[機能]

静的マルチホーミングの削除

[入力形式]

remote [<number>] multihoming static delete <count>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

削除する静的マルチホーミング情報の定義番号を指定します。

- 削除する転送可否定義番号
  削除する静的マルチホーミング情報の定義番号を指定します。
- all
  すべての静的マルチホーミング情報を削除する場合に指定します。

[説明]

指定した静的マルチホーミング情報を削除します。

5.7.14　remote multihoming alive

[機能]

WAN 側セッション経路監視の設定

[入力形式]

remote [<number>] multihoming alive <dst_addr> [<resend_time> [<time_out> [<normal_interval> [<error_interval>]]]]

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<dst_addr>

- ICMP ECHO パケットの宛先 IP アドレス
  WAN 側セッションの経路を監視するために実行する ICMP ECHO パケットの宛先 IP アドレスを指定します。
  0.0.0.0 を指定した場合は、WAN 側セッション経路を監視しません。

<resend_time>

- ICMP ECHO パケットの再送間隔
  ICMP ECHO パケットの再送間隔を、1 秒～60 秒の範囲で指定します。
  単位は、m(分)、s(秒) のいずれかを指定します。
  省略した場合は、5 秒を指定したものとみなされます。

<time_out>

- ICMP ECHO のタイムアウト時間
  ICMP ECHO のタイムアウト時間を、<resend_time>+1 秒～240 秒の範囲で指定します。
  単位は、m(分)、s(秒) のいずれかを指定します。
  省略した場合は、<resend_time>× 3 ＋ 1 秒を指定したものとみなされます。

<normal_interval>

- ICMP ECHO パケットの正常時送信間隔
  ICMP ECHO パケットの正常時送信間隔を、<time_out>+1 秒～255 秒の範囲で指定します。
  単位は、m(分)、s(秒) のいずれかを指定します。
  省略した場合は、<time_out>+1 秒を指定したものとみなされます。

<error_interval>

- ICMP ECHO パケットの異常時送信間隔
  ICMP ECHO パケットの異常時送信間隔を、1 秒～255 秒の範囲で指定します。
  単位は、m(分)、s(秒) のいずれかを指定します。
  省略した場合は、30 秒を指定したものとみなされます。

[説明]

WAN 側セッションの経路を監視するための動作情報を設定します。
<dst_addr>で指定した宛先に ICMP ECHO パケットを送出し、<time_out>時間応答がない場合、WAN 側経路がダウンしたものとみなされます。

[未設定時]

WAN 側セッション経路を監視しないものとみなされます。

```
remote <number> multihoming alive 0.0.0.0 5s 16s 17s 30s
```

5.8　フレームリレー関連情報

5.8.1　remote fr dlci

[機能]

フレームリレーにおける DLCI の設定

[入力形式]

remote [<number>] fr dlci <dlci_number>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<dlci_number>

- DLCI
  自局で使用する DLCI を、16～991 の 10 進数値で指定します。
  なお、設定を削除する場合は、0 を指定します。

[説明]

フレームリレーにおける DLCI(データリンクコネクション識別子) を設定します。
フレームリレーを使用する場合は、本コマンドを必ず実行してください。

[未設定時]

DLCI を設定しないものとみなされます。

5.8.2 remote fr cir

[機能]

フレームリレーにおける CIR の設定

[入力形式]

remote [<number>] fr cir <cir>

[パラメタ]

<number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<cir>

- CIR 値
  CIR 値を、0〜アクセス速度 / 2 で指定します。

[説明]

フレームリレーにおける、DLCI ごとの CIR 値 (認定情報速度) を設定します。

[未設定時]

CIR 値として 0 を指定したものとみなされます。

```
remote <number> fr cir 0
```

第 6 章　着信デフォルト情報の設定

6.1　発信者番号 (CLID) で相手が判別できないときの着信動作情報

6.1.1　answer accept

[機能]

発信者番号非通知または発信者番号非登録相手からの着信動作の設定

[入力形式]

answer accept <mode>

[パラメタ]

<mode>

- enable
  着信を受け付けます。
- disable
  着信を受け付けません。

[説明]

発信者番号 (CLID) が通知されない着信、または “5.2.26 remote ap called number” で設定したいずれの番号とも一致しない着信について、着信を許可するかどうかを設定します。

[未設定時]

着信を受け付けないものとみなされます。

```
answer accept disable
```

6.1.2 answer callback

[機能]

コールバック応答動作の設定

[入力形式]

answer callback <mode> [<kind> <time>]

[パラメタ]

<mode>

- enable
  着信時にコールバックを行います。
- disable
  着信時にコールバックを行いません。

以下のパラメタは<mode>が disable の場合は省略することができます。

<kind>

- cbcp
  コールバック方式として「CBCP 方式」を指定します。

<time>

- コールバック待ち時間
  コールバック要求着信を受理したあと、相手にコールバック応答発信を行うまでの待ち時間を、0 秒～60 秒の範囲で指定します。
  単位は、m(分)、s(秒) のいずれかを指定します。

[説明]

発信者番号 (CLID) が通知されない着信、または remote ap called number で設定したいずれの番号とも一致しない着信について、コールバック応答するかどうかを設定します。

[未設定時]

着信時にコールバック応答動作を行わないものとみなされます。

```
answer callback disable
```

6.1.3　answer ppp auth type

[機能]

着信認証方式の設定

[入力形式]

answer ppp auth type <authtype>

[パラメタ]

<authtype>

着信時の認証について指定します。

- off
  着信時の認証を行いません。
- pap
  着信時の認証プロトコルに PAP を使用します。
- chap_md5
  着信時の認証プロトコルに MD5-CHAP を使用します。
- any
  着信時の認証プロトコルに MD5-CHAP または PAP を使用します。

[説明]

着信時の認証方式を設定します。

[未設定時]

着信時の認証プロトコルに MD5-CHAP または PAP を用います。

```
answer ppp auth type any
```

6.1.4 answer ppp auth receive add

[機能]

受諾認証情報の設定

[入力形式]

answer ppp auth receive add <id> <password> [encrypted]

[パラメタ]

<id>

- 受諾認証 ID
  受諾認証 ID を、0x21,0x23～0x7e のコードで構成される 64 文字以内の ASCII 文字列で指定します。

<password>

- 受諾認証パスワード
  受諾認証パスワードを、0x21,0x23～0x7e のコードで構成される 64 文字以内の文字列で指定します。
- 暗号化された受諾認証パスワード
  show コマンドで表示される暗号化された受諾認証パスワードを encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

<encrypted>

- 暗号化受諾認証パスワード
  <password>に暗号化された受諾認証パスワードを設定する場合に指定します。

[説明]

受諾認証情報を設定します。
受諾認証 ID、受諾認証パスワードを設定します。この認証 ID、認証パスワードは以下の場合に使用されます。

- 発信者番号 (CLID) で相手が判別できた場合
  その相手に対する認証 ID、認証パスワードがない場合における共通認証 ID、パスワードとして利用されます。
- 発信者番号 (CLID) で相手が判別できなかった場合
  不特定相手着信として着信を許可するための認証 ID、パスワードとして利用されます。

[注意]

show コマンドでは、暗号化された受諾認証パスワードが encrypted と共に表示されます。

[未設定時]

受諾認証 ID は定義されません。

6.1.5　answer ppp auth receive delete

[機能]

受諾認証情報の削除

[入力形式]

answer ppp auth receive delete <id>

[パラメタ]

<id>

- 受諾認証 ID
  削除する受諾認証 ID を指定します。
- all
  すべての受諾認証 ID を削除対象とします。

[説明]

受諾認証情報を削除します。

6.1.6 answer ppp mp use

[機能]

着信時の MP 利用可否の設定

[入力形式]

answer ppp mp use <mode>

[パラメタ]

<mode>

MP を利用するかどうかを指定します。

- off
  MP を利用しない場合に指定します。
- on
  MP を利用する場合に指定します。

[説明]

発信者番号 (CLID) で相手が判別できない着信について、MP を利用するかどうかを設定します。

[未設定時]

MP を利用しないものとみなされます。

```
answer ppp mp use off
```

6.1.7　answer ppp mp bap use

[機能]

着信時の BAP/BACP 利用可否の設定

[入力形式]

answer ppp mp bap use <mode>

[パラメタ]

<mode>

BAP/BACP を利用するかどうかを指定します。

- off
  BAP/BACP を利用しない場合に指定します。
- on
  BAP/BACP を利用する場合に指定します。

[説明]

発信者番号 (CLID) で相手が判別できない着信について、BAP/BACP を利用するかどうかを設定します。

[未設定時]

BAP/BACP を利用しないものとみなされます。

```
answer ppp mp bap use off
```

6.2 不特定相手着信の動作情報

6.2.1 answer ppp compress

[機能]

データ圧縮機能の設定

[入力形式]

answer ppp compress <mode>

[パラメタ]

<mode>

- off
  データ圧縮機能を使用しない場合に指定します。
- on
  データ圧縮機能を使用する場合に指定します。

[説明]

データ圧縮機能を使用するかどうか設定します。

[未設定時]

データ圧縮機能を使用しないものとみなされます。

```
answer ppp compress off
```

6.2.2　answer ppp mp start

[機能]

MP 利用時における初期接続リンク数の設定

[入力形式]

answer ppp mp start <link>

[パラメタ]

<link>

- MP 利用時の初期接続リンク数
  MP 利用時の初期接続リンク数を、1～2 の 10 進数値で指定します。

[説明]

MP 利用時の初期接続リンク数を設定します。
コールバック応答発信時かつ MP 利用時において、最初から接続を試みるリンク数を設定します。発信に失敗した場合の再試行は行いません。

[未設定時]

初期接続リンク数として 1 を設定したものとみなされます。

```
answer ppp mp start 1
```

6.2.3 answer ppp mp resource analog

[機能]

アナログ発着信時の縮退動作の設定

[入力形式]

answer ppp mp resource analog <mode>

[パラメタ]

<mode>

- on
  アナログ発着信時に縮退動作を行います。
- off
  アナログ発着信時に縮退動作を行いません。

[説明]

MP 接続時に、アナログ発着信による縮退動作を行うかどうかを設定します。

[注意]

着信において縮退を行う場合には、「通信中着信通知」の契約が必要です。

[未設定時]

アナログ発着信時に縮退動作を行わないものとみなされます。

```
answer ppp mp resource analog off
```

6.2.4　answer ppp mp traffic use

[機能]

自動チャネル数制御の可否の設定

[入力形式]

answer ppp mp traffic use <mode>

[パラメタ]

<mode>

- on
  スループット BOD の機能を使用します。
- off
  スループット BOD の機能を使用しません。

[説明]

スループット BOD 機能を使用するかどうかを設定します。

[未設定時]

スループット BOD 機能を使用しないとみなされます。

```
answer ppp mp traffic use off
```

6.2.5 answer ppp mp traffic increase

[機能]

リンク増加閾値の設定

[入力形式]

answer ppp mp traffic increase <traffic> <time>

[パラメタ]

<traffic>

- 回線増加閾値

  単位時間当たりにおけるチャネル利用率を、0～100 の 10 進数値で指定します。

  以下に、回線増加閾値の計算式を示します。

  チャネル利用率 (%) = 転送バイト量 ÷ 転送可能バイト数 × 100

<time>

- 増加猶予時間

  トラフィックが回線増加閾値を超え続けた場合に、発信するまでの猶予時間を、0 秒～3600 秒の範囲で指定します。

  単位は、m(分)、s(秒) のいずれかを指定します。

[説明]

スループット BOD 機能使用時におけるリンク増加閾値を設定します。
スループット BOD 機能を使用する場合は、本コマンドを必ず設定してください。

[注意]

指定した増加猶予時間の間、チャネル利用率が回線増加閾値を超え続けた場合にチャネル増加のための発信が行われます。

[未設定時]

回線増加閾値および猶予時間を設定しないものとみなされます。

6.2.6　answer ppp mp traffic decrease

[機能]

リンク減少閾値の設定

[入力形式]

answer ppp mp traffic decrease <traffic> <time>

[パラメタ]

<traffic>

- 回線減少閾値

  単位時間当たりにおけるチャネル利用率を、0～100 の 10 進数値で指定します。

  以下に、回線減少閾値の計算式を示します。

  チャネル利用率 (%) = 転送バイト量 ÷ 転送可能バイト数 × 100

<time>

- 減少猶予時間

  トラフィックが回線減少閾値を超え続けた場合に、切断するまでの猶予時間を、0 秒～3600 秒の範囲で指定します。

  単位は、m(分)、s(秒) のいずれかを指定します。

[説明]

スループット BOD 利用時におけるリンク減少閾値を設定します。
スループット BOD 機能を使用する場合は、本コマンドを必ず設定してください。

[注意]

設定された減少猶予時間の間、チャネル利用率が回線減少閾値を下回り続けた場合にチャネル減少が行われます。

[未設定時]

回線減少閾値および猶予時間を設定しないものとみなされます。

6.2.7 answer ppp mp order

[機能]

受信パケット順序制御の有無の設定

[入力形式]

answer ppp mp order <mode>

[パラメタ]

<mode>

- off
  順序制御をしない場合に指定します。
- on
  順序制御をする場合に指定します。

[説明]

MP 受信パケットの順序制御を行うかどうか設定します。

[注意]

以下に、MP 受信パケットの順序制御が無効になっていると動作に影響が出る機能を示します。

- VJ ヘッダ圧縮機能
  設定にかかわらず、常に VJ ヘッダ圧縮を使用しません。
- IP ヘッダ圧縮機能
  設定にかかわらず、常に IP ヘッダ圧縮を使用しません。
- データ圧縮機能
  LZS アルゴリズムで、ヒストリ機能 (高効率圧縮の機能) を使用しません。

[未設定時]

MP 受信パケットの順序制御をしないものとみなされます。

```
answer ppp mp order off
```

6.2.8　answer ppp ipcp vjcomp

[機能]

VJ-Compression の利用の有無の設定

[入力形式]

answer ppp ipcp vjcomp <mode>

[パラメタ]

<mode>

- enable
  VJ ヘッダ圧縮を使用する場合に指定します。
- disable
  VJ ヘッダ圧縮を使用しない場合に指定します。

[説明]

VJ ヘッダ圧縮機能 (VJCOMP) を使用するかどうかを設定します。VJ ヘッダ圧縮機能は、RFC1144 に準拠しています。

[注意]

MP を使用する場合は、answer ppp mp order の<mode>に on を指定して、受信順序制御を使用してください。
MP を使用するにもかかわらず受信順序制御を使用しないと定義している場合、VJ ヘッダ圧縮機能は無条件に無効となります。

[未設定時]

VJ ヘッダ圧縮機能を使用するものとみなされます。

```
answer ppp ipcp vjcomp enable
```

6.2.9 answer ppp ipcp iphc

[機能]

IPv4 における IP ヘッダ圧縮 (IPHC) の設定

[入力形式]

answer ppp ipcp iphc <mode>

[パラメタ]

<mode>

- enable
  IP ヘッダ圧縮を使用する場合に指定します。
- disable
  IP ヘッダ圧縮を使用しない場合に指定します。

[説明]

IPv4 において、IP ヘッダ圧縮 (IPHC) を使用するかどうかを設定します。IP ヘッダ圧縮機能は、圧縮方法が RFC2507 / RFC2508 に、ネゴシエーション方法が RFC2509 に準拠しています。

[注意]

MP を使用する場合は、remote ppp mp order の<mode>に on を指定して、受信順序制御を使用してください。
MP を使用するにもかかわらず受信順序制御を使用しないと定義している場合、IP ヘッダ圧縮機能は無条件に無効となります。

[未設定時]

IP ヘッダ圧縮機能を使用しないものとみなされます。

```
answer ppp ipcp iphc disable
```

6.2.10　answer ip address pool

[機能]

発信者番号非通知または発信者番号非登録相手に割り当てる IP アドレス範囲の設定

[入力形式]

answer ip address pool <start> <num>

[パラメタ]

<start>

- 割り当て先頭アドレス
  割り当てる IP アドレスの先頭アドレスを指定します。

<num>

- 割り当てアドレス数
  (1 または 2)

[説明]

発信者番号 (CLID) が通知されない着信、または remote ap called number で設定したいずれの番号とも一致しない着信相手に対して、割り当てる IP アドレスの範囲を指定します。

[未設定時]

割り当てる IP アドレス範囲を設定しないものとみなされます。

6.2.11 answer ip filter

[機能]

IP フィルタの設定

[入力形式]

answer ip filter <count> <action> <src_addr> / <mask> <src_port> <dst_addr> / <mask> <dst_port> <protocol> <tcpconnect> [<tos>]

[パラメタ]

<count>

- フィルタリング定義番号
  フィルタリングの優先度を表す番号を、0〜63 の 10 進数値で指定します。
  指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つフィルタリング定義がすでに存在する場合は、既存の定義を変更します。

<action>

パケットを透過するかどうかを設定します。

- pass
  条件と一致する場合に、パケットを透過します。
- reject
  条件と一致する場合に、パケットを遮断します。
- restrict
  条件と一致した場合に、回線が接続されていれば透過させ、切断されていれば遮断します。

<src_addr>/<mask>

入力フィルタリングの対象となる IP アドレス、マスクビット数を指定します。

- IP アドレス / マスクビット数 (またはマスク値)
  入力フィルタリングの対象となる IP アドレスとマスクビット数の組み合わせを指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。
  以下に、有効な記述形式を示します。
  - IP アドレス / マスクビット数 (例: 192.168.1.1 / 24)
  - IP アドレス / マスク値 (例: 192.168.1.1 / 255.255.255.0)
- any
  すべての IP アドレスを対象とする場合に指定します。
  0.0.0.0 / 0(0.0.0.0 / 0.0.0.0) を指定するのと同じ意味になります。

<src_port>

入力フィルタリングの対象となるポート番号を指定します。

- ポート番号
  入力フィルタリングの対象となるポート番号を、1〜65535 の 10 進数値で指定します。複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、
  範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。
  ポート番号は、","(カンマ) または"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。
  以下に、有効な記述形式を示します。

- 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
- ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
- ポート番号- (例: 1- = 1 から 65535 までのポート)
- -ポート番号 (例: -1000 = 1 から 1000 までのポート)
- ポート番号, ポート番号 … (例: 10,20,30- = 10 と 20 と 30 以降のポート)

- any
  すべてのポート番号を対象とする場合に指定します。

<dst_addr>/<mask>

出力フィルタリングの対象となる IP アドレス、マスクビット数を指定します。

- IP アドレス / マスクビット数 (またはマスク値)
  出力フィルタリングの対象となる IP アドレスとマスクビット数の組み合わせを指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。
  以下に、有効な記述形式を示します。
  IP アドレス / マスクビット数 (例: 192.168.1.1 / 24)
  IP アドレス / マスク値 (例: 192.168.1.1 / 255.255.255.0)
- any
  すべての IP アドレスを対象とする場合に指定します。
  0.0.0.0 / 0(0.0.0.0 / 0.0.0.0) を指定するのと同じ意味になります。

<dst_port>

出力フィルタリングの対象となるポート番号を指定します。

- ポート番号
  出力フィルタリングの対象となるポート番号を、1〜65535 の 10 進数値で指定します。複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。
  ポート番号は、","(カンマ) または"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。
  以下に、有効な記述形式を示します。
  - 1〜65535 の 10 進数値 (例: 65535 = 65535 ポート)
  - ポート番号-ポート番号 (例: 32-640 = 32 から 640 までのポート)
  - ポート番号- (例: 1- = 1 から 65535 までのポート)
  - -ポート番号 (例: -1000 = 1 から 1000 までのポート)
  - ポート番号, ポート番号 … (例: 10,20,30- = 10 と 20 と 30 以降のポート)
- any
  すべてのポート番号を対象とする場合に指定します。

<protocol>

- プロトコル番号
  フィルタリング対象のプロトコル番号を、0〜255 の 10 進数値で指定します (例: ICMP:1、TCP:6、UDP:17 など)。
  0 を指定した場合は、すべてのプロトコルが対象となります。

<tcpconnect>

- yes
  TCP の場合に、SYN flag だけが立つパケットを対象に含めます。
- no
  TCP の場合に、SYN flag だけが立つパケットを対象に含めません。

<tos>

フィルタリングの対象となる TOS 値を指定します。

- フィルタリング対象 TOS 値
  フィルタリング対象の TOS 値を、0～ff の 16 進数値で指定します。
  複数の TOS 値を指定する場合は、","(カンマ) で区切って指定します。また、範囲指定する場合は、"-"(ハイフン) を使用して指定します。
  TOS 値は、","(カンマ) または"-"(ハイフン) を使用して 10 個まで指定できます。
- any
  すべての TOS 値を対象とする場合に指定します。

省略した場合は、any を指定したものとみなされます。

[説明]

不特定相手着信のインタフェースに対する IP フィルタを設定します。
IP フィルタリング定義は、本装置全体で 64 個まで定義できます。

[注意]

IP フィルタは、インタフェースの入力/出力方向にプロトコル、アドレス、ポート番号を設定し、パケットを透過 (pass) するか、遮断 (reject) するかを指定します。

[未設定時]

IP フィルタリングは行わないとみなされます。すべてのパケットが透過されます。

6.2.12　answer ip filter move

[機能]

IP フィルタの優先順序の変更

[入力形式]

answer ip filter move <count> <new_count>

[パラメタ]

<count>

- 対象フィルタリング定義番号
  優先順序を変更するフィルタリング定義の番号を指定します。

<new_count>

- 移動先フィルタリング定義番号
  <count>に対する新しい順序を、0～63 の 10 進数値で指定します。
  すでにこの番号を持つ定義が存在する場合には、その定義の前に挿入されます。

[説明]

IP フィルタの優先順序を変更します。

6.2.13 answer ip filter delete

[機能]

IP フィルタの削除

[入力形式]

answer ip filter delete <count>

[パラメタ]

<count>

削除するフィルタリングを指定します。

- 削除するフィルタリング定義番号
  削除するフィルタリングの定義番号を指定します。
- all
  すべてのフィルタリングを削除する場合に指定します。

[説明]

IP フィルタを削除します。

6.2.14　answer ip dns

[機能]

DNS サーバアドレスの設定

[入力形式]

answer ip dns <dns>

[パラメタ]

<dns>

- DNS サーバアドレス
  相手装置に通知する DNS サーバアドレスを指定します。
  0.0.0.0 を指定した場合は通知しません。

[説明]

相手装置から IPCP 機能を用いて DNS サーバアドレス通知要求を受けた場合に、<dns>で設定した IP アドレスを通知します。本コマンドによる設定がない場合は通知しません。

[未設定時]

DNS サーバアドレスの通知を行わないものとみなされます。

```
answer ip dns 0.0.0.0
```

6.2.15 answer ip tos

[機能]

TOS 値書き換え条件の設定

[入力形式]

answer ip tos <count> <src_addr>/<mask> <src_port> <dst_addr>/<mask> <dst_port> <protocol> <tos> <new_tos>

[パラメタ]

<count>

- TOS 値書き換え定義番号
  TOS 値書き換え対象の定義番号として、0～31 の 10 進数値を指定します。
  指定した値は、設定完了時に順方向にソートされてリナンバリングされます。
  また、指定した定義番号と同じ値を持つ TOS 値書き換え定義がすでに存在する場合は、既存定義の値を変更します。

<src_addr>/<mask>

- any
  すべてのアドレスを TOS 値書き換えの対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<src_port>

TOS 値書き換え対象となる送信元ポート番号を指定します。

- ポート番号
  TOS 値書き換え対象となる送信元ポート番号を、1～65535 の 10 進数値で指定します。
  複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。
  また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。
  ポート番号は、","(カンマ) または"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。・any すべてのポート番号を対象とする場合に指定します。

<dst_addr>/<mask>

TOS 値書き換え対象となる宛先 IP アドレス、マスクビット数を指定します。

- 宛先 IP アドレス/マスクビット数 (またはマスク値)
  TOS 値書き換え対象となる宛先 IP アドレスとマスクビット数の組み合わせを指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。
- any
  すべてのアドレスを TOS 値書き換えの対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<dst_port>

TOS 値書き換え対象となる宛先ポート番号を指定します。

- ポート番号
  TOS 値書き換え対象となる宛先ポート番号を、1～65535 の 10 進数値で指定します。
  複数のポート番号を指定する場合は、","(カンマ) で区切って指定します。
  また、範囲指定する場合は、「1000-1200」のように"-"(ハイフン) を使用して指定します。
  ポート番号は、","(カンマ) または"-"(ハイフン) を使用して、<src_port>、<dst_port>合わせて 10 個まで指定できます。
- any
  すべてのポート番号を対象とする場合に指定します。

<protocol>

- プロトコル番号
  TOS 値書き換え対象のプロトコル番号を、0～255 の 10 進数値で指定します
  (例: ICMP:1、TCP:6、UDP:17 など)。
  0 を指定した場合は、すべてのプロトコルが対象となります。

<tos>

- 書き換え対象 TOS 値
  書き換え対象 TOS 値を、0～ff の 16 進数値で指定します。範囲指定する場合は、「0-ff」のように"-"(ハイフン) を使用して指定します。また、複数指定する場合は、","(カンマ) を区切りとして 10 個まで指定できます。
- any
  すべての TOS 値を、TOS 値書き換えの対象とする場合に指定します。

<new_tos>

- 書き換え TOS フィールド値
  書き換え TOS フィールド値を、0～ff の 16 進数値で指定します。

[説明]

TOS 値書き換え条件を設定します。条件に一致したパケットの TOS 値を、指定した値に書き換えます。
TOS 値書き換え定義は、本装置全体で最大 32 個まで定義できます。

[未設定時]

TOS 値書き換えを行わないものとみなされます。

6.2.16 answer ip tos move

[機能]

TOS 値書き換え条件の優先順序の変更

[入力形式]

answer ip tos move <count> <new_count>

[パラメタ]

<count>

- 対象 TOS 値書き換え定義番号
  優先順序を変更する前の TOS 値書き換え定義番号を指定します。

<new_count>

- 移動先 TOS 値書き換え定義番号
  <count>に対して、新しい順序を指定します。

すでにこの番号を持つ定義が存在する場合には、その定義の前に挿入されます。

[説明]

TOS 値書き換え条件の優先順序を変更します。

6.2.17　answer ip tos delete

[機能]

TOS 値書き換え条件の削除

[入力形式]

answer ip tos delete <count>

[パラメタ]

<count>

削除する TOS 値書き換え定義を指定します。

- TOS 値書き換え定義番号
  削除する TOS 値書き換え定義番号を指定します。
- all
  すべての TOS 値書き換え定義を削除する場合に指定します。

[説明]

TOS 値書き換え条件を削除します。

6.2.18 answer idle

[機能]

無通信監視タイマの設定

[入力形式]

answer idle <time>

[パラメタ]

<time>

- 無通信監視時間
  無通信監視時間を、0 秒～3600 秒の時間で指定します。
  単位は、h(時)、m(分)、s(秒) のいずれかを指定します。
  0 秒を指定した場合は、監視を行いません。

[説明]

不特定相手と接続した場合の無通信監視時間を設定します。

[未設定時]

無通信監視を行わないものとみなされます。

```
answer idle 0d
```

第 7 章　RADIUS 情報の設定

7.1　RADIUS 情報

7.1.1　radius service

[機能]

RADIUS サービスの設定

[入力形式]

radius service <service>[,<service>]

[パラメタ]

<service>

- auth
  RADIUS による認証を使用します。
- account
  RADIUS によるアカウント (課金) を使用します。
- off
  RADIUS サービスをすべて使用しません。

[説明]

使用する RADIUS サービスを設定します。
RADIUS 認証と RADIUS アカウントは独立して設定でき、動作させることができます。
<service>に"auth"を指定した場合、RADIUS 認証サーバと認証用 RADIUS シークレットを別途設定する必要があります。
<service>に"account"を指定した場合、RADIUS アカウントサーバとアカウント用 RADIUS シークレットを別途設定する必要があります。

[未設定時]

RADIUS サービスをすべて使用しないものとみなされます。

```
radius service off
```

7.1.2 radius auth server

[機能]

RADIUS 認証サーバの設定

[入力形式]

radius auth server <address>

[パラメタ]

<address>

- RADIUS 認証サーバアドレス
  RADIUS 認証を行うサーバの IP アドレスを指定します。
  0.0.0.0 を指定した場合は、RADIUS 認証サーバアドレスを削除します。

[説明]

RADIUS 認証サーバの IP アドレスを設定します。複数サーバを指定することはできません。

[未設定時]

RADIUS 認証サーバアドレスを設定しないものとみなされます。

7.1.3　radius auth secret

[機能]

認証用 RADIUS シークレットの設定

[入力形式]

設定:
radius auth secret <secret> [encrypted]
設定の削除:
radius auth secret

[パラメタ]

<secret>

- RADIUS シークレット
  本装置と RADIUS 認証サーバとの間で取り決めたシークレット文字列を、0x21,0x23～0x7e の 64 文字以内の ASCII 文字で指定します。
- 暗号化された RADIUS シークレット
  show コマンドで表示される暗号化された RADIUS シークレットを encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定します。

encrypted

- 暗号化 RADIUS シークレット指定
  <secret>に暗号化された RADIUS シークレットを指定する場合に指定します。

[説明]

RADIUS 認証サーバと共有する RADIUS シークレット文字列を設定します。
show コマンドでは、暗号化された RADIUS シークレットが encrypted と共に表示されます。
show radius auth secret を実行すると、暗号化していない RADIUS シークレットが表示されます。

[未設定時]

認証用 RADIUS シークレットを設定しないものとみなされます。

7.1.4 radius account server

[機能]

RADIUS アカウントサーバの設定

[入力形式]

radius account server <address>

[パラメタ]

<address>

- RADIUS アカウントサーバアドレス
  RADIUS アカウントを行うサーバの IP アドレスを指定します。
  RADIUS 認証サーバと同じ RADIUS サーバの場合は、RADIUS 認証サーバと同じアドレスを指定します。
  0.0.0.0 を指定した場合は、RADIUS アカウントサーバアドレスを削除します。

[説明]

RADIUS アカウントサーバの IP アドレスを設定します。複数サーバを指定することはできません。

[未設定時]

RADIUS アカウントサーバの IP アドレスを設定しないものとみなされます。

7.1.5　radius account secret

[機能]

アカウント用 RADIUS シークレットの設定

[入力形式]

設定:
radius account secret <secret> [encrypted]
設定の削除:
radius account secret

[パラメタ]

<secret>

- RADIUS シークレット
  本装置と RADIUS アカウントサーバとの間で取り決めたシークレット文字列を、0x21, 0x23～0x7e の 64 文字以内の ASCII 文字で指定します。
- 暗号化された RADIUS シークレット
  show コマンドで表示される暗号化された RADIUS シークレットを encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定します。

encrypted

- 暗号化 RADIUS シークレット指定
  <secret>に暗号化された RADIUS シークレットを指定する場合に指定します。

[説明]

RADIUS アカウントサーバと共有する RADIUS シークレット文字列を設定します。
show コマンドでは、暗号化された RADIUS シークレットが encrypted と共に表示されます。
show radius account secret を実行すると、暗号化していない RADIUS シークレットが表示されます。

[未設定時]

アカウント用 RADIUS シークレットは設定しないものとみなされます。

第 8 章　ルーティングプロトコル情報の設定

8.1　ルーティングマネージャ情報

8.1.1　routemanage distance

[機能]

IPv4 ルーティングプロトコル優先度の設定

[入力形式]

routemanage distance rip <rip_distance>
routemanage distance bgp <external_distance>

[パラメタ]

<rip_distance>

- RIP で受信した経路情報の優先度
  設定可能範囲は 1～254 です。

<external_distance>

- E-BGP で受信した経路情報の優先度
  設定可能範囲は 1～254 です。

[説明]

複数の IPv4 ルーティングプロトコルで同じ経路情報を受信した場合、どのプロトコルで受信した情報を優先的に使用するかを、各経路情報に設定されている優先度で判断します。本コマンドでは、各経路情報に対する優先度を設定します。なお、優先度は小さい方が高い優先度を示します。

[未設定時]

<rip_distance>が 120、<external_distance>が 20 とみなされます。

```
routemanage distance rip 120
routemanage distance bgp 20
```

8.1.2　routemanage redist

[機能]

IPv4 ルーティングプロトコル再広報の設定

[入力形式]

routemanage redist rip <redist_info> <mode> [<metric>]
routemanage redist bgp <redist_info> <mode>

[パラメタ]

<redist_info>

- static
  本装置に設定されているスタティックルーティングの経路情報を示します。本パラメタは、routemanage redist rip または routemanage redist bgp で指定可能です。
- connected
  インタフェースが接続されているネットワークの経路情報を示します。本パラメタは、routemanage redist bgp で指定可能です。なお、RIP では本情報が常に広報され、広報しないように設定することはできません。
- bgp
  BGP で受信した経路情報を示します。本パラメタは、routemanage redist rip で指定可能です。

<mode>

- off
  <redist_info>で指定した経路情報を広報しません。
- on
  <redist_info>で指定した経路情報を広報します。

<metric>

- RIP で広報するメトリック値
  RIP で広報する際のメトリック値を示します。本パラメタは、routemanage redist rip で設定可能です。ただし、<redist_info>に"static"を指定した場合、本パラメタを指定できません。設定可能範囲は 0～16 です。RIP 広報メトリック値は、以下の計算値で決定されます。
  - RIP 広報値=インタフェースの加算メトリック値+1+<metric>

[説明]

IPv4 ルーティングプロトコル (RIP / BGP) で広報する経路情報の種別を設定します。
routemanage redist bgp static on を設定し、スタティックルーティング情報と同じ宛先の経路情報を BGP で受信した場合、スタティックルーティング情報を優先します。
routemanage redist bgp on を設定し、スタティックルーティング情報で設定したデフォルトルートを BGP で広報する場合は、bgp neighbor default-originate コマンドで on を指定し、デフォルトルートを広報する設定を行ってください。off が設定されている場合、デフォルトルートは広報されません。

[未設定時]

以下の設定とみなされます。

- RIP で static を広報する
- RIP で bgp を広報しない
- BGP で static を広報しない

- BGP で connected を広報しない

```
routemanage redist rip static on
routemanage redist rip bgp off 0
routemanage redist bgp static off
routemanage redist bgp connected off
```

8.2　BGP 情報

8.2.1　bgp as

[機能]

BGP AS 番号の設定

[入力形式]

bgp as <as_number>

[パラメタ]

<as_number>

- 自装置の属する AS 番号
  設定可能範囲は 0～65535 です。
  0 を指定した場合、BGP の機能は動作しません。

[説明]

自装置の属する AS 番号を指定します。

[未設定時]

BGP を動作させないものとみなされます。

```
bgp as 0
```

8.2.2 bgp id

[機能]

BGP ID の設定

[入力形式]

bgp id <identifier>

[パラメタ]

<identifier>

- BGP を使用するルータを特定するための ID
  IPv4 アドレスで指定します。

[説明]

自装置を一意に示す ID を設定します。設定する ID は、ほかのルータと重複しない ID をドット形式で指定します。一般的には自装置の IP アドレス (IPv4) を設定します。0.0.0.0 を指定すると、自装置のインタフェースに設定されている IP アドレスの中でもっとも大きな値を ID として使用します。

[未設定時]

自装置のインタフェースに設定されている IP アドレスの中でもっとも大きな値を使用するものとみなされます。

```
bgp id 0.0.0.0
```

8.2.3　bgp network

[機能]

BGP 広報ネットワークの設定

[入力形式]

bgp network <count> <address>/<mask> <action>

[パラメタ]

<count>

- 広報するネットワークの定義番号
  設定可能範囲は 0～15(定義数は最大 16) です。

<address>/<mask>

- IPv4 アドレス/マスクビット数 (またはマスク値)
  広報するネットワークの IPv4 アドレスとマスクビット数の組み合わせを指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。以下に、有効な記述形式を示します。
  - IPv4 アドレス/マスクビット数 (例: 192.168.1.0/24)
  - IPv4 アドレス/マスク値 (例: 192.168.1.0/255.255.255.0)
    0.0.0.0/0, 0.0.0.0/0.0.0.0 および、<address>と<mask>の論理積が 0 になる値は指定できません。

<action>

- always-only
  <address>/<mask>で指定したネットワークを常に広報します。このネットワークの範囲に含まれる広報すべき経路情報が存在しても、それらの個別経路情報については広報しません。
- always-both
  <address>/<mask>で指定したネットワークを常に広報します。このネットワークの範囲に含まれる広報すべき経路情報が存在する場合、それらの経路情報についても広報します。
- exist-only
  <address>/<mask>で指定したネットワークの範囲に含まれる広報すべき経路が存在する場合のみ、<address>/<mask>で指定したネットワークを広報します。<address>/<mask>で指定したネットワークの範囲に含まれる広報すべき経路情報が存在しても、それらの個別経路情報については広報しません。
- exist-both
  <address>/<mask>で指定したネットワークの範囲に該当する広報すべき経路情報が存在する場合のみ、<address>/<mask>で指定したネットワークを広報します。この経路情報の範囲に含まれる広報すべき経路情報が存在する場合、それらの個別経路情報についても広報します。

[説明]

相手装置に広報するネットワークと広報する形態を設定します。
<address>/<mask>パラメタでは、広報する BGP 経路情報を指定します。
デフォルトルートは設定できません。
<action>パラメタでは、指定した BGP 広報ネットワークの広報形態を指定します。<action>パラメタは以下の 2 つの要素の組み合わせを表現したものです。

- 常に広報するかどうか

  always :　<address>/<mask>で指定したネットワークを常に広報します。

exist : <address>/<mask>で指定したネットワークの範囲に含まれる BGP で広報すべき個別経路が存在する場合のみ、<address>/<mask>で指定したネットワークを広報します。

- 集約前の経路を広報するかどうか

  only : <address>/<mask>で指定したネットワークのみを広報し、その範囲に含まれる個別経路情報は広報しません。

  both : <address>/<mask>で指定したネットワークに加え、その範囲に含まれる個別経路も広報します。

BGP 広報ネットワークでは、routemanage redist コマンドで BGP へ広報する設定をしたものが対象となります。なお、RIP の経路情報は対象にはなりません。

[注意]

本コマンドで設定した経路情報よりも、長いネットマスクの経路情報は受信しません。

[未設定時]

相手装置に広報するネットワークを設定しないものとみなされます。

8.2.4　bgp network delete

[機能]

BGP 広報ネットワークの削除

[入力形式]

bgp network delete <count>

[パラメタ]

<count>

- 広報するネットワークの定義番号
  設定可能範囲は 0～15(定義数は最大 16) です。
- all
  すべての設定を削除します。

[説明]

相手装置に広報するネットワークを削除します。

8.3 BGP 相手側情報

8.3.1 bgp neighbor address

[機能]

BGP 相手側 IP アドレスの設定

[入力形式]

bgp neighbor <count> address <address>

[パラメタ]

<count>

- 相手装置の定義番号
  0 を指定します。

<address>

- 相手装置の IPv4 アドレス
  設定値として、0.0.0.0 および 255.255.255.255 は使用できません。

[説明]

相手装置の定義番号および IPv4 アドレスを設定します。相手側情報の設定では、まず本コマンドを実行し、定義番号と IPv4 アドレスを設定しなければなりません。
<address>には、IP-VPN 網の契約でのキャリア側 IP アドレスを設定してください。

[未設定時]

相手側情報を設定しないものとみなされます。

8.3.2　bgp neighbor delete

[機能]

BGP 相手側情報の削除

[入力形式]

bgp neighbor delete <count>

[パラメタ]

<count>

- 相手装置の定義番号
  0 を指定します。
- all
  すべての定義を削除します。

[説明]

相手側情報を削除します。
bgp neighbor の定義のすべて (address, as, timers, medmetric, asprepend, ebgp-multihop, default-originate の設定) が削除されます。

8.3.3 bgp neighbor as

[機能]

BGP 相手側 AS 番号の設定

[入力形式]

bgp neighbor <count> as <as_number>

[パラメタ]

<count>

- 相手装置の定義番号
  0 を指定します。

<as_number>

- 相手装置の所属する AS 番号
  設定可能範囲は 1～65535 です。

[説明]

相手装置の属する AS 番号を設定します。
自装置の属する AS 番号とは異なる値を設定しなければなりません。本装置で I-BGP は使用できません。

[未設定時]

相手装置の AS 番号を設定していないものとみなされます。

8.3.4　bgp neighbor timers

[機能]

BGP 無通信監視タイマの設定

[入力形式]

bgp neighbor <count> timers <keepalive> <holdtime>

[パラメタ]

<count>

- 相手装置の定義番号
  0 を指定します。

<keepalive>

- keepalive タイマ値
  設定可能範囲は 1 秒～65535 秒です。
  単位は、h(時)、m(分)、s(秒) のいずれかを指定します。
  各単位での設定可能範囲は、1s～65535s、1m～1092m、1h～18h です。

<holdtime>

- HoldTime のタイマ値 (秒)
  設定可能範囲は 3 秒～65535 秒です。
  単位は、h(時)、m(分)、s(秒) のいずれかを指定します。
  各単位での設定可能範囲は、3s～65535s、1m～1092m、1h～18h です。

[説明]

<keepalive>では、無通信状態において、相手装置との通信可否を確認するために送信する KEEPALIVE メッセージのタイマ値を設定します。相手装置の<holdtime>が自装置の<holdtime>よりも小さな値が設定されている場合、相手装置の<holdtime>の 3 分の 1 の値が使用されます。
<holdtime>では無通信状態で通信異常と判断する時間を設定します。本値は相手装置とネゴシエーションし、より小さな値をお互いの装置で使用します。
<keepalive>には<holdtime>よりも小さな値を指定してください。
<holdtime>と<keepalive>の設定値は、上位単位で表示可能な場合、上位単位で表示されます。

[未設定時]

<keepalive>に 30 秒、<holdtime>に 90 秒を設定するものとみなされます。

```
bgp neighbor 0 timers 30s 90s
```

8.3.5 bgp neighbor medmetric

[機能]

BGP MED メトリックの設定

[入力形式]

bgp neighbor <count> medmetric <medmetric>

[パラメタ]

<count>

- 相手装置の定義番号
  0 を指定します。

<medmetric>

- 相手装置に広報する MED メトリック値
  設定可能範囲は 0～4294967295 です。
  本パラメタ値は、小さい値がより高い優先度を示します。

[説明]

相手装置に広報する MED メトリック値を指定します。<medmetric>に 0 以外を指定した場合、相手装置に広報する経路情報すべてに対して MED メトリック値を広報します。<medmetric>に 0 を指定した場合、MED メトリック値として 0 を広報します。

[未設定時]

MED メトリック値として 0 を広報するものとみなされます。

```
bgp neighbor 0 medmetric 0
```

8.3.6　bgp neighbor asprepend

[機能]

BGP AS パスプリペンドの設定

[入力形式]

bgp neighbor <count> asprepend <asprepend>

[パラメタ]

<count>

- 相手装置の定義番号
  0 を指定します。

<asprepend>

- AS 番号の追加数
  設定可能範囲は 0～4 です。

[説明]

相手装置に E-BGP で広報する AS 番号の個数を追加します。
<asprepend>で 0 を指定した場合は、広報される AS 番号は、自 AS 番号のみの 1 個として扱われます。

[未設定時]

広報する AS 番号の個数を追加しないとみなされます。

```
bgp neighbor 0 asprepend 0
```

8.3.7 bgp neighbor ebgp-multihop

[機能]

EBGP マルチホップの設定

[入力形式]

bgp neighbor <count> ebgp-multihop <ttl>

[パラメタ]

<count>

- 相手装置の定義番号
  0 を指定します。

<ttl>

- TTL 値
  設定可能範囲は 1～255 です。

[説明]

直接接続していない相手装置と E-BGP 接続する場合に必要なホップ数 (IP パケットの TTL 値) を設定します。

[未設定時]

<ttl>に 1 を設定するものとみなされます。

```
bgp neighbor 0 ebgp-multihop 1
```

8.3.8　bgp neighbor default-originate

[機能]

BGP デフォルトルート広報可否の設定

[入力形式]

bgp neighbor <count> default-originate <mode>

[パラメタ]

<count>

- 相手装置の定義番号
  0 を指定します。

<mode>

- off
  デフォルトルートを広報しません。
- on
  デフォルトルートを広報します。

[説明]

デフォルトルートを広報するかどうかを設定します。
<mode>に off を設定した場合、広報する経路情報にデフォルトルートがあっても広報しません。<mode>に on を設定した場合、広報する経路情報にデフォルトルートがあるときは広報します。

[未設定時]

<mode>に off を設定するものとみなされます。

```
bgp neighbor 0 default-originate off
```

第 9 章　ブリッジ情報の設定

9.1　ブリッジ情報

9.1.1　bridge age

[機能]

ブリッジ学習テーブルの生存時間の設定

[入力形式]

bridge age <age_time>

[パラメタ]

<age_time>

- 生存時間
  MAC アドレス学習によって学習した情報の生存時間を、10 秒～1000000 秒の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。

[説明]

本コマンドは、ブリッジ機能を使用する場合にだけ有効です。
アドレス学習テーブルの生存時間を設定します。
アドレス学習機能によって学習された MAC アドレステーブルを最後に使用してから削除されるまでの時間を設定します。

[未設定時]

アドレス学習テーブルの生存時間として 5 分を定義するものとみなされます。

```
bridge age 5m
```

9.1.2　bridge stp priority

[機能]

ブリッジ優先度の設定

[入力形式]

bridge stp priority <priority>

[パラメタ]

<priority>

- 優先度
  ブリッジネットワーク内での本装置の優先度を、0～65535 の 10 進数値で指定します。値が小さいほど、優先度が高くなります。

[説明]

本コマンドは、STP を使用する場合にだけ有効です。
ルートブリッジ決定アルゴリズムで使用するブリッジの優先度を指定します。一般的なブリッジネットワークではルートブリッジにトラフィックが集中するため、バックボーンに近いブリッジが優先となるように設定してください。ルートブリッジにするブリッジには、最小の値を指定してください。

[未設定時]

優先度として 32768 を定義するものとみなされます。

```
bridge stp priority 32768
```

9.1.3 bridge stp age

[機能]

Hello メッセージ待ち時間の設定

[入力形式]

bridge stp age <max_age>

[パラメタ]

<max_age>

- 待ち時間
  ルートブリッジから送出される構成情報 BPDU の待ち時間を、6 秒～40 秒の範囲で指定します。
  単位は、s(秒) を指定します。

[説明]

本コマンドは、STP を使用する場合にだけ有効です。
ルートブリッジまたは代表ブリッジから送出される構成情報 BPDU の待ち時間を指定します。

[未設定時]

待ち時間に 20 秒を設定したものとみなされます。

```
bridge stp age 20s
```

9.1.4　bridge stp hello

[機能]

Hello メッセージ送出間隔の設定

[入力形式]

bridge stp hello <time>

[パラメタ]

<time>

- 送出間隔
  ルートブリッジになったときに定期的に送出する構成情報 BPDU の送出間隔の時間を、1 秒～10 秒の範囲で指定します。単位は、s(秒) を指定します。

[説明]

本コマンドは、STP を使用する場合にだけ有効です。
本装置がルートブリッジとなったときに送出する構成情報 BPDU の送出間隔を指定します。
STP を使用する場合でも、本装置がルートブリッジとならなかった場合は、設定が無効となります。

[未設定時]

送出間隔に 2 秒を設定したものとみなされます。

```
bridge stp hello 2s
```

9.1.5 bridge stp delay

[機能]

最大中継遅延時間の設定

[入力形式]

bridge stp delay <delay_time>

[パラメタ]

<delay_time>

- 最大中継遅延時間
  最大中継遅延時間を、4 秒～30 秒の範囲で指定します。単位は、s(秒) を指定します。

[説明]

本コマンドは、STP を使用する場合にだけ有効です。
最大中継遅延時間を設定します。
STP を使用する場合でも、本装置がルートブリッジとならなかった場合は、設定が無効となります。
STP で Listening 状態から Learning 状態に変化する場合、または Learning 状態から Forwarding 状態に変化するまでの時間 (ルートブリッジから広報される時間) を指定します。

[未設定時]

最大中継遅延時間に 15 秒を設定したものとみなされます。

```
bridge stp delay 15s
```

第 10 章　VPN 情報の設定

10.1　IPsec 情報

IPsec の Main Mode を使用する場合の設定を行います。IPsec の Aggressive Mode を使用する場合は、remote ap ipsec type を参照してください。

10.1.1　ipsec delete

[機能]

IPsec 情報の削除

[入力形式]

ipsec delete <number>

[パラメタ]

<number>

削除する IPsec 情報を指定します。

- IPsec 定義番号
  IPsec 定義番号を、0～63 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。
- all
  すべての IPsec 定義番号を削除対象とします。

[説明]

<number>で指定した IPsec 情報を削除します。

10.1.2 ipsec move

[機能]

IPsec 情報の定義順序の変更

[入力形式]

ipsec move <number> <new_number>

[パラメタ]

<number>

- IPsec 定義番号
  移動元の IPsec 定義番号を、0～63 の範囲の 10 進数値を指定します。

<new_number>

- IPsec 定義番号
  移動先の IPsec 定義番号を、0～63 の範囲の 10 進数値を指定します。

[説明]

IPsec 情報の定義順序を変更します。

10.1.3　ipsec range

[機能]

IPsec 情報の対象範囲の設定

[入力形式]

ipsec [<number>] range <src_addr> / <mask> <dst_addr> / <mask>

[パラメタ]

<number>

- IPsec 定義番号
  IPsec 定義番号を、0〜63 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<src_addr>/<mask>

IPsec 対象となる送信元 IP アドレスとマスクビット数を指定します。

- IP アドレス / マスクビット数 (またはマスク値)
  IPsec 対象となる送信元 IP アドレスとマスクビット数の組み合わせを指定します。マスクビット数は 0〜32(10 進数) が入力可能です。
  例) IPv4: 192.168.1.1 / 24
- any4
  すべての IPv4 アドレスを IPsec 対象に含めます。
  0.0.0.0 / 0(0.0.0.0 / 0.0.0.0) と同意。

<dst_addr>/<mask>

IPsec 対象となる宛先 IP アドレスとマスクビット数を指定します。

- IP アドレス / マスクビット数 (またはマスク値)
  IPsec 対象となる宛先 IP アドレスとマスクビット数の組み合わせを指定します。マスクビット数は 0〜32(10 進数) が入力可能です。
  例) IPv4: 192.168.1.1 / 24

[説明]

IPsec を適用するセッションの範囲を設定します。(Security Policy Database の情報)
IPsec 情報は、手動鍵設定と自動鍵設定 (交換) を合わせて、装置に 63 個設定することが可能です。
1 つのトンネル (双方向で IPsec を行う) を張るためには、IPsec 情報を入力用と出力用を対にして定義してください。
<src_addr> / <dst_addr>の any4 指定は、手動鍵設定のときにのみ有効です。

[注意]

手動鍵設定と自動鍵設定 (交換) について

- 手動鍵設定と自動鍵設定 (交換) の識別方法
  「ipsec path」で path の直後に現れる<spi>に、文字列"ike"が指定されていた場合、その定義を自動鍵設定 (交換) と判断します。
  手動鍵設定を行う場合に、自動鍵設定 (交換) で使用する定義を行っても使用されません。

- 自動鍵設定 (交換) の定義について
  以下のコマンドは、IKE(ISAKMP) で ISAKMP SA および IPsec SA の確立および更新に使用される定義です。
  ipsec path ike ... と定義した場合に使用されます。
  - ipsec pfs
  - ipsec lifetime
  - ipsec lifebyte
  - ipsec newsa initiator
  - ipsec newsa responder
  - ike remote address
  - ike remote port
  - ike remote shared key
  - ike remote proposal encrypt
  - ike remote proposal hash
  - ike remote proposal pfs
  - ike remote proposal lifetime
  - ike remote retry
  - ike remote release

[未設定時]

IPsec 情報の range 設定は設定されません。IPsec を使用する場合は必ず設定してください。

10.1.4　ipsec path

[機能]

IPsec 情報の区間の設定

[入力形式]

ipsec [<number>] path <spi> <src_addr> <dst_addr>

[パラメタ]

<number>

- IPsec 定義番号
  IPsec 定義番号を、0～63 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<spi>

- セキュリティパラメタインデックス (SPI)
  セキュリティパラメタインデックスを、16 進数値で指定します。(0x100～0xffffffff の 16 進数)
  ただし、自動鍵設定 (交換) を使用する場合は、文字列で"ike"と指定します。

<src_addr>

- IPsec 対象パケットをセキュア化する送信元 IP アドレスを指定します。
  例) IPv4: 192.168.1.1

<dst_addr>

- IPsec 対象パケットをアンセキュア化する宛先 IP アドレスを指定します。
  指定方法は<src_addr>参照。

[説明]

IPsec 対象パケットがセキュア化される区間を設定します。(Security Association Database の情報)

[注意]

<src_addr>の 0.0.0.0/0 指定は、手動鍵設定のときにのみ有効です。自動鍵設定の場合に指定すると正しく動作しません。

[未設定時]

IPsec 対象パケットがセキュア化される区間を定義していないものとみなされます。
IPsec を使用する場合は必ず設定してください。

10.1.5 ipsec encrypt

[機能]

IPsec 情報の暗号情報の設定

[入力形式]

ipsec [<number>] encrypt <enc_algo>[,<enc_algo>...] [<kind> <enc_key> [encrypted]]

[パラメタ]

<number>

- IPsec 定義番号
  IPsec 定義番号を、0～63 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<enc_algo>

暗号アルゴリズムを指定します。
自動鍵設定として定義する場合は、複数のアルゴリズムを指定することができます。複数定義するときは、アルゴリズムを空白なしでカンマ',' で区切ります。(暗号アルゴリズム定義とセキュリティプロトコルの関係は [説明] を参照)

- des-cbc
- 3des-cbc
- null
- none

<kind>

鍵種別を指定します。

- hex
  16 進数鍵
- text
  文字列鍵

<enc_key>

暗号鍵を指定します。

鍵種別 暗号アルゴリズム	hex 16進数鍵	text 文字列鍵
des-cbc 3des-cbc	1～16桁 1～48桁	8文字 24文字

- 暗号化されていない暗号鍵
  <enc_algo>で指定した暗号アルゴリズムが使用する鍵長未満の鍵を指定した場合は、16 進数鍵では鍵長になるまで"0"でパディングされます。
  文字列鍵の場合は、0x22(ダブルクォーテーション) を除く [0x20-0x7e] の範囲のコードで構成される ASCII 文字列で指定します。ただし、文字列鍵で 0x20(空白文字) を使用する場合には、文字列鍵を""で囲う必要があります。
  以下に、入力範囲を示します。
- 暗号化された暗号鍵
  暗号化された暗号鍵を指定します。
  show コマンドで表示される暗号化された暗号鍵を encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化暗号鍵指定

  <enc_key>に暗号化された暗号鍵を指定する場合に指定します。

[説明]

送受信パケットを暗号化／復号化するための、暗号アルゴリズムと鍵の設定を行います。
show コマンドでは、暗号化された暗号鍵が encrypted と共に表示されます。
show ipsec [<number>] encrypt を実行すると、暗号化していない暗号鍵が表示されます。

表 10.1　認証／暗号アルゴリズム定義とセキュリティプロトコルの関係

auth(認証)	encrypt(暗号)	セキュリティプロトコル
―	―	ESP(null encrypt)
○	―	AH(認証)
―	○	ESP(暗号)
○	○	ESP(認証 + 暗号)

○:定義あり ―:定義なし

- 手動鍵設定としての暗号アルゴリズム

  暗号アルゴリズムが"none"または"null"の場合、暗号鍵は入力できません。

- 自動鍵設定としての暗号アルゴリズム

  暗号鍵は自動生成されるので、設定は不要です。

  暗号アルゴリズムを複数指定する場合、指定順序にかかわらず以下の優先順位となります。

  1. 3des-cbc
  2. des-cbc
  3. null

[注意]

- 暗号アルゴリズムの複数指定は、自動鍵設定のみの機能なので、暗号アルゴリズムの複数指定と、暗号鍵を同時に指定することはできません。

  認証／暗号アルゴリズムの未定義は、認証アルゴリズムを"none"、暗号アルゴリズムを"null"と指定した場合と同じ動作となります。

- weak key

  手動鍵設定で指定する暗号鍵では、RFC2409 の Appendix A に記載されている weak key を指定できません。

```
RFC2409のAppendix Aに記載されているweak key

0101010101010101, FEFEFEFEFEFEFEFE, 1F1F1F1FE0E0E0E0, E0E0E0E01F1F1F1F,
01FE01FE01FE01FE, FE01FE01FE01FE01, 1FE01FE00EF10EF1, E01FE01FF10EF10E,
01E001E001F101F1, E001E001F101F101, 1FFE1FFE0EFE0EFE, FE1FFE1FFE0EFE0E,
011F011F010E010E, 1F011F010E010E01, E0FEE0FEF1FEF1FE, FEE0FEE0FEF1FEF1
```

  3des-cbc の場合は、暗号鍵を 16 桁ごとに 3 つの鍵に分割し、いずれかの鍵が weak key となるような指定はできません。

[未設定時]

暗号アルゴリズムを指定しないものとみなされます。

```
ipsec <number> encrypt none
```

10.1.6　ipsec auth

[機能]

IPsec 情報の認証情報の設定

[入力形式]

ipsec [<number>] auth <auth_algo>[,<auth_algo>...] [<kind> <auth_key> [encrypted]]

[パラメタ]

<number>

- IPsec 定義番号

  IPsec 定義番号を、0～63 の 10 進数値で指定します。

  省略した場合は、0 を指定したものとみなされます。

<auth_algo>

認証アルゴリズムを指定します。

自動鍵設定として定義する場合は、複数のアルゴリズムを指定することができます。複数定義するときは、アルゴリズムを空白なしでカンマ',' で区切ります。(認証アルゴリズム定義とセキュリティプロトコルの関係は、「ipsec encrypt コマンドの [説明]」を参照)

- hmac-md5
- hmac-sha1
- none

<kind>

鍵種別を指定します。

- hex

  16 進数鍵

- text

  文字列鍵

<auth_key>

認証鍵を指定します。

鍵種別 認証アルゴリズム	hex 16 進数鍵	text 文字列鍵
hmac-md5	1～32 桁	16 文字
hmac-sha1	1～40 桁	20 文字

- 暗号化されていない認証鍵

  <auth_algo>で指定した認証アルゴリズムが使用する鍵長未満の鍵を指定した場合は、16 進数鍵では鍵長になるまで"0"でパディングされます。

  文字列鍵の場合は、0x22(ダブルクォーテーション) を除く [0x20-0x7e] の範囲のコードで構成される ASCII 文字列で指定します。ただし、文字列鍵で 0x20(空白文字) を使用する場合には、文字列鍵を""で囲う必要があります。以下に、入力範囲を示します。

- 暗号化された認証鍵を指定します。

  show コマンドで表示される暗号化された認証鍵を encrypted と共に指定します。

  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化認証鍵指定
  <auth_key>に暗号化された認証鍵を指定する場合に指定します。

[説明]

送受信パケットを認証するための、認証アルゴリズムと鍵の設定を行います。
show コマンドでは、暗号化された認証鍵が encrypted と共に表示されます。
show ipsec [<number>] encrypt を実行すると、暗号化していない認証鍵が表示されます。

- 手動鍵設定としての認証アルゴリズム
  認証アルゴリズムが"none"の場合、認証鍵を省略することができます。
- 自動鍵設定としての認証アルゴリズム
  認証鍵は自動生成されるので、設定は不要です。
  認証アルゴリズムを複数指定する場合、指定順序にかかわらず以下の優先順位となります。

  1. hmac-md5
  2. hmac-sha1

[注意]

認証アルゴリズムの複数指定は、自動鍵設定のみの機能なので、認証アルゴリズムの複数指定と、認証鍵を同時に指定することはできません。

[未設定時]

認証アルゴリズムを指定しないものとみなされます。

```
ipsec <number> auth none
```

10.1.7　ipsec pfs

[機能]

IPsec 情報の PFS グループの設定

[入力形式]

ipsec [<number>] pfs <pfs_group>

[パラメタ]

<number>

- IPsec 定義番号
  IPsec 定義番号を、0〜63 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<pfs_group>

Diffie-Hellman グループについて指定します。

- modp768
  Diffie-Hellman グループの MODP768
- modp1024
  Diffie-Hellman グループの MODP1024
- off
  Diffie-Hellman グループを使用しません。

[説明]

IPsec で使用する鍵の交換データを保護する、PFS グループの設定を行います。PFS グループを使用する場合、MODP1024 が強い暗号強度となりますが処理に時間がかかりますので、ネゴシエーション時間が長くなります。

[注意]

PFS グループに off を指定した場合、PFS による鍵交換データ保護は行いません。
セキュア通信を行いたい場合は適切な PFS グループを設定してください。

[未設定時]

PFS グループに Diffie-Hellman のグループを使用しないものとみなされます。

```
ipsec <number> pfs off
```

10.1.8 ipsec lifetime

[機能]

IPsec 情報の SA 有効時間の設定

[入力形式]

ipsec [<number>] lifetime <lifetime>

[パラメタ]

<number>

- IPsec 定義番号
  IPsec 定義番号を、0～63 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<lifetime>

- SA 有効時間
  IPsec 用 Security Association(SA) 有効時間を、600 秒 (10 分)～86400 秒 (1 日) の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。

[説明]

IPsec セッションの通信データを保護する、IPsec SA の SA 有効時間の設定を行います。

[未設定時]

SA 有効時間に 8 時間を指定したものとみなされます。

```
ipsec <number> lifetime 8h
```

10.1.9　ipsec lifebyte

[機能]

IPsec 情報の SA 有効パケット量の設定

[入力形式]

ipsec [<number>] lifebyte <lifebyte>

[パラメタ]

<number>

- IPsec 定義番号
  IPsec 定義番号を、0～63 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<lifebyte>

- SA 有効パケット量
  IPsec 用 Security Association(SA) 有効パケット量のバイト数を、0 または 2400k～108000m の範囲で指定します。
  単位は以下の 3 種類です。1k は 1024 バイトで計算されます。
  k: キロバイト (例: 2400k → 2400k)
  m: メガバイト (例: 4m → 4096k)
  g: ギガバイト (例: 1g → 1048576k)
  0 を指定した場合は、lifebyte による IPsec SA の更新を行いません。

[説明]

IPsec セッションの通信データを保護する、IPsec SA の SA 有効パケット量 (キロバイト) の設定を行います。

[未設定時]

SA 有効パケット量に 0 バイトを指定したものとみなされます。

```
ipsec <number> lifebyte 0
```

10.1.10 ipsec newsa initiator

[機能]

IPsec 情報の New SA Initiator(更新時間) の設定

[入力形式]

ipsec [<number>] newsa initiator <time>

[パラメタ]

<number>

- IPsec 定義番号
  IPsec 定義番号を、0～63 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time>

- Initiator SA 更新時間
  Initiator SA 更新時間を、30 秒～180 秒 (3 分) の範囲で指定します。単位は、m(分)、s(秒) のいずれかを指定します。

[説明]

自側が Initiator の場合に、IPsec SA の有効時間が満了になる前に、IPsec SA の更新を行うための時間の設定を行います。
相手側の New SA Responder と同じ時間にならないように設定してください。

[未設定時]

Initiator SA 更新時間に 90 秒を指定したものとみなされます。

```
ipsec <number> newsa initiator 90s
```

10.1.11　ipsec newsa responder

[機能]

IPsec 情報の New SA Responder(更新時間) の設定

[入力形式]

ipsec [<number>] newsa responder <time>

[パラメタ]

<number>

- IPsec 定義番号
  IPsec 定義番号を、0～63 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time>

- Responder SA 更新時間
  Responder SA 更新時間を、30 秒～180 秒 (3 分) の範囲で指定します。
  単位は、m(分)、s(秒) のいずれかを指定します。

[説明]

自側が Responder の場合に、IPsec SA の有効時間が満了になる前に、IPsec SA の更新を行うための時間の設定を行います。

[未設定時]

Responder SA 更新時間に 30 秒を指定したものとみなされます。

```
ipsec <number> newsa responder 30s
```

10.2 IKE 情報

10.2.1 ike remote delete

[機能]

IKE 情報の削除

[入力形式]

ike remote delete <ike_number>

[パラメタ]

<ike_number>

- IKE 定義番号
  IPsec 定義番号を、0～31 の 10 進数値で指定します。
- all
  すべての IKE 定義番号を削除対象とします。

[説明]

<ike_number>で指定した IKE 情報を削除します。IKE 情報を削除しても<ike_number>のソートはしません。

10.2.2　ike remote address

[機能]

IKE 情報の宛先アドレスの設定

[入力形式]

ike remote [<ike_number>] address <address>

[パラメタ]

<ike_number>

- IKE 定義番号
  IPsec 定義番号を、0～31 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<address>

- 宛先アドレス
  相手装置のアドレスを指定します。0.0.0.0 が設定された場合は、定義なしとなります。

[説明]

IKE セッションを確立する、相手装置の IP アドレスの設定を行います。

[未設定時]

IKE 情報の宛先アドレスは設定されていないものとみなされます。
IKE により鍵交換を行う場合は必ず設定してください。

10.2.3 ike remote port

[機能]

IKE 情報の相手側 IKE ポート番号の設定

[入力形式]

ike remote [<ike_number>] port <port>

[パラメタ]

<ike_number>

- IKE 定義番号
  IPsec 定義番号を、0～31 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<port>

- 相手側 IKE(ISAKMP) ポート番号
  相手側 IKE(ISAKMP) ポート番号を指定します。(デフォルト: 500 番)

[説明]

SA 確立のネゴシエーションを行う、相手側 IKE(ISAKMP) サーバのポート番号の設定を行います。

[未設定時]

相手側 IKE(ISAKMP) ポート番号に標準ポート番号である 500 を指定したものとみなされます。

```
ike remote <ike_number> port 500
```

10.2.4　ike remote shared key

[機能]

IKE セッション確立時の共通鍵 (Pre-shared key) の設定

[入力形式]

ike remote [<ike_number>] shared key <kind> <shared_key> [encrypted]

[パラメタ]

<ike_number>

- IKE 定義番号
  IPsec 定義番号を、0～31 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<kind>

鍵種別を指定します。

- hex
  16 進数鍵
- text
  文字列鍵

<shared_key>

認証鍵を指定します。

- 暗号化されていない共通鍵を指定します。
  文字列鍵の場合は、0x22(ダブルクォーテーション) を除く [0x20-0x7e] の範囲のコードで構成される ASCII 文字列で指定します。ただし、文字列鍵で 0x20(空白文字) を使用する場合には、文字列鍵を""で囲う必要があります。以下に、入力範囲を示します。

16 進数鍵	文字列鍵
1～256 桁	1 文字～128 文字

- 暗号化された共通鍵を指定します。
  show コマンドで表示される暗号化された共通鍵を encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化共通鍵指定
  <shared_key>に暗号化された共通鍵を指定する場合に指定します。

[説明]

SA 確立のネゴシエーションのときに接続相手を認証するための、共通鍵の設定を行います。
show コマンドでは、暗号化された共通鍵が encrypted と共に表示されます。
show ike remote [<ike_number>] shared key を実行すると、暗号化していない認証鍵が表示されます。

[未設定時]

IKE セッション確立時の共通鍵 (Pre-shared key) は設定されていないものとみなされます。
IKE により鍵交換を行う場合は必ず設定してください。

10.2.5 ike remote proposal delete

[機能]

IKE 情報の Proposal 定義の削除

[入力形式]

ike remote [<ike_number>] proposal delete <count>

[パラメタ]

<ike_number>

- IKE 定義番号
  IKE 定義番号を、0～31 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

削除する Proposal 定義を指定します。

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。
- all
  <ike_number>で指定した IKE 情報のすべての Proposal 定義を削除対象とします。

[説明]

<ike_number>で指定した IKE 情報の<count>で指定される Proposal 定義または、すべての Proposal 定義を削除します。

10.2.6　ike remote proposal move

[機能]

IKE セッション用 Proposal 定義優先順序の変更

[入力形式]

ike remote <ike_number> proposal move <count> <new_count>

[パラメタ]

<ike_number>

- IKE 定義番号
  IKE 定義番号を、0～31 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- Proposal 定義番号
  移動元の Proposal 定義優先順序を指定します。

<new_count>

- Proposal 定義番号
  移動先の Proposal 定義優先順序を指定します。

[説明]

<ike_number>で指定した IKE セッション用の Proposal 定義優先順序を変更します。

表 10.2　IKE セッション用 Proposal 定義とネゴシエーションの関係

	ネゴシエーション情報	Proposal	Proposal	...
a	暗号情報	3des-cbc	des-cbc	...
b	ハッシュ情報	hmac-md5	0	...
c	PFS グループ	modp768	modp1024	...
d	SA 有効時間	600s	0	...

※ a を複数指定 (<count>0,1,2 を定義) した場合、ほかの情報は定義しなければ各情報のデフォルト値を採用します。
IKE セッションのネゴシエーションは、Proposal 単位 (a～d を一組) として行います。その中で a～c は相手装置の定義と一致することが条件となります。
複数定義した場合の<count>が 1 以降の定義は、Main モードで自側が Initiator の場合に使用されます。
自側が Responder の場合は、相手の Proposal が許容できるかを判断するため、自装置の定義は参照されません。

10.2.7 ike remote proposal encrypt

[機能]

IKE セッション用暗号情報の設定

[入力形式]

ike remote <ike_number> proposal [<count>] encrypt <enc_algo>

[パラメタ]

<ike_number>

- IKE 定義番号
  IKE 定義番号を、0～31 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。省略された場合は"0"と解釈します。

<enc_algo>

- 暗号アルゴリズム
  暗号アルゴリズムを指定します。
  des-cbc
  3des-cbc

[説明]

IKE セッションの送受信パケットを暗号化／復号化するための、暗号アルゴリズムの設定を行います。

[未設定時]

暗号アルゴリズムは設定されていないものとみなされます。
IKE により鍵交換を行う場合は必ず設定してください。

10.2.8　ike remote proposal hash

[機能]

IKE セッション用ハッシュ情報の設定

[入力形式]

ike remote <ike_number> proposal [<count>] hash <hash_algo>

[パラメタ]

<ike_number>

- IKE 定義番号
  IKE 定義番号を、0～31 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。省略された場合は"0"と解釈します。

<hash_algo>

ハッシュアルゴリズムを指定します。

- hmac-md5
- hmac-sha1

[説明]

IKE セッションのネゴシエーションパケットを認証するための、ハッシュアルゴリズムの設定を行います。

[未設定時]

ハッシュアルゴリズムに hmac-md5 を指定したものとみなされます。

```
ike remote <ike_number> proposal hash hmac-md5
```

10.2.9 ike remote proposal pfs

[機能]

IKE セッション用 PFS グループの設定

[入力形式]

ike remote <ike_number> proposal [<count>] pfs <pfs_group>

[パラメタ]

<ike_number>

- IKE 定義番号
  IKE 定義番号を、0～31 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。省略された場合は"0"と解釈します。

<pfs_group>

Diffie-Hellman グループについて指定します。

- modp768
  Diffie-Hellman グループの MODP768
- modp1024
  Diffie-Hellman グループの MODP1024

[説明]

IKE セッションのネゴシエーションパケットを保護するための、PFS グループの設定を行います。

[未設定時]

PFS グループに modp768 を指定したものとみなされます。

```
ike remote <ike_number> proposal pfs modp768
```

10.2.10　ike remote proposal lifetime

[機能]

IKE 用 SA 有効時間の設定

[入力形式]

ike remote <ike_number> proposal [<count>] lifetime <lifetime>

[パラメタ]

<ike_number>

- IKE 定義番号
  IKE 定義番号を、0～31 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<count>

- Proposal 定義番号
  Proposal 定義番号として 0-2 の範囲の 10 進数値を指定します。省略された場合は"0"と解釈します。

<lifetime>

- IKE 用 Security Association(SA) 有効時間
  SA 有効時間の時間を、600 秒 (10 分)～86400 秒 (1 日) の範囲で指定します。単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。

[説明]

IKE セッションのネゴシエーションパケットを保護する SA の有効時間 (秒) の設定を行います。

[未設定時]

IKE SA 有効時間に 1 日 (24 時間) を指定したものとみなされます。

```
ike remote <ike_number> proposal lifetime 1d
```

10.2.11 ike remote retry

[機能]

IKE 情報の初回再送時間 (再送時間) および再送回数の設定

[入力形式]

ike remote <ike_number> retry <time> <count>

[パラメタ]

<ike_number>

- IKE 定義番号
  IKE 定義番号を、0～31 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<time>

- 初回再送時間
  初回再送時間を、1 秒～60 秒 (1 分) の範囲で指定します。単位は、m(分)、s(秒) のいずれかを指定します。

<count>

- 再送回数
  再送回数を、1～10 の範囲で指定します。

[説明]

IKE セッションのネゴシエーションパケットに対する再送時間および再送回数の設定を行います。

[未設定時]

IKE 情報の初回再送時間に 10 秒、再送回数設定に 3 回を指定したものとみなされます。

```
ike remote <ike_number> retry 10s 3
```

10.2.12　ike remote release

[機能]

IPsec / IKE 情報の解放動作の設定

[入力形式]

ike remote [<ike_number>] release <mode>

[パラメタ]

<ike_number>

- IKE 定義番号
  IKE 定義番号を、0〜31 の 10 進数値で指定します。
  省略した場合は、0 を指定したものとみなされます。

<mode>

IPsec / IKE の SA 情報の解放動作設定を指定します。

- on
  回線切断時に解放処理を行います。
- off
  解放処理は行いません。

[説明]

自動鍵設定で作成された SA 情報の解放動作を設定します。
on を指定した場合は、回線切断時に自動鍵設定が使用している SA 情報の解放動作を行います。
off を指定した場合は、回線切断時に自動鍵設定が使用している SA 情報の解放動作を行いません。

[注意]

本コマンドは以下の回線切断動作時に有効です。

- ISDN(回線交換) を使用したとき

[未設定時]

回線切断時に IKE SA 情報の解放動作を行うものとみなされます。

```
ike remote <ike_number> release on
```

第 11 章　装置情報の設定

11.1　SNMP 情報

11.1.1　snmp service

[機能]

SNMP エージェント機能および SNMP トラップ機能の設定

[入力形式]

snmp service <mode>

[パラメタ]

<mode>

- on
  SNMP エージェント機能および SNMP トラップ機能を有効にします。
- off
  SNMP エージェント機能および SNMP トラップ機能を停止します。

[説明]

SNMP エージェント機能および SNMP トラップ機能を有効にするかどうかを設定します。

[未設定時]

SNMP エージェント機能を停止するとみなされます。

```
snmp service off
```

11.1.2　snmp agent contact

[機能]

SNMP エージェント機能でのルータ管理者の設定

[入力形式]

snmp agent contact [<syscontact>]

[パラメタ]

<syscontact>

- ルータ管理者 (sysContact 値)
  本装置の管理者を表す MIB 変数 sysContact を、40 文字以内で指定します。
  省略した場合は、設定を削除します。

[説明]

SNMP エージェント機能でのルータ管理者を設定します。

[未設定時]

ルータ管理者を設定しないものとみなされます。

11.1.3 snmp agent sysname

[機能]

SNMP エージェント機能での機器名称の設定

[入力形式]

snmp agent sysname [<sysname>]

[パラメタ]

<sysname>

- 機器名称 (sysName 値)
  本装置の機器名称を表す MIB 変数 sysName を、32 文字以内で指定します。
  省略した場合は、設定を削除します。

[説明]

SNMP エージェント機能での機器名称を設定します。

[未設定時]

機器名称を設定しないものとみなされます。

11.1.4　snmp agent location

[機能]

SNMP エージェント機能での機器設置場所の設定

[入力形式]

snmp agent location [<syslocation>]

[パラメタ]

<syslocation>

- 機器設置場所 (sysLocation 値)
  本装置の管理者を表す MIB 変数 sysLocation を、72 文字以内で指定します。
  省略した場合は、設定を削除します。

[説明]

SNMP エージェント機能での機器設置場所を設定します。

[未設定時]

機器設置場所を設定しないものとみなされます。

11.1.5 snmp agent address

[機能]

SNMP エージェントアドレスの設定

[入力形式]

snmp agent address [<address>]

[パラメタ]

<address>

- エージェントアドレス
  本装置のエージェントアドレスを設定します。
  0.0.0.0 を指定した場合は、SNMP エージェントアドレスを削除します。

[説明]

SNMP エージェントのアドレスを設定します。本設定は TRAP 送信時の自局アドレスにも使用されます。
SNMP エージェント機能を使用する場合は、必ず設定してください。

[未設定時]

エージェントアドレスを設定しないものとみなされます。その場合、MIB 情報の通知パケットおよび
TRAP パケットの自局 IP アドレスは不定となります。

11.1.6　snmp manager

[機能]

SNMP ホスト情報の設定

[入力形式]

snmp manager <manager_number> <address> <community> <trap> [<write>]

[パラメタ]

<manager_number>

- SNMP ホスト定義番号
  SNMP ホスト定義の通し番号を、0〜1 の 10 進数値で指定します。

<address>

- アクセス許可 / トラップ送信アドレス
  アクセス許可およびトラップを送信する宛先 IP アドレスを、XXX.XXX.XXX.XXX(XXX は 3 桁の 10 進数値) の形式で指定します。
  0.0.0.0 を指定すると、すべてのホストからのアクセスを許可し、trap 送信は行いません。

<community>

コミュニティ名を指定します。

- コミュニティ名
  トラップを送信するときのコミュニティ名を、1〜32 文字で指定します。
- public
  任意の SNMP マネージャと通信する場合に指定します。

<trap>

トラップ送信するかどうかを指定します。

- on
  トラップ送信する場合に指定します。
- off
  トラップ送信しない場合に指定します。

<write>

SNMP マネージャからの書き込みを許可するかどうか指定します。

- enable
  SNMP マネージャからの書き込みを許可する場合に指定します。
- disable
  SNMP マネージャからの書き込みを許可しない場合に指定します。

省略した場合は、disable を指定したものとみなされます。

[説明]

SNMP ホストの情報を設定します。

[未設定時]

SNMP ホストの情報を設定しないものとみなされます。

11.1.7 snmp manager delete

[機能]

SNMP ホスト情報の削除

[入力形式]

snmp manager delete <manager_number>

[パラメタ]

<manager_number>

- SNMP ホスト定義番号
  削除する SNMP ホスト定義の通し番号を、0～1 の 10 進数値で指定します。
- all
  すべての SNMP ホスト定義番号を削除する場合に指定します。

[説明]

SNMP ホスト情報を削除します。

11.2　システムログ情報

11.2.1　syslog server

[機能]

システムログ情報の受信サーバの設定

[入力形式]

syslog server [<address>]

[パラメタ]

<address>

- IP アドレス
  システムログ情報 (メッセージ) を受信するサーバの IP アドレスを指定します。省略した場合は、設定を削除します。

[説明]

システムログ情報 (メッセージ) を受信するサーバを設定します。
以下に、システムログ情報の出力方法を示します。

1) “syslog server <address>” で設定した IP アドレスのホストに送信する。
2) dsplog コマンドで表示する。

[未設定時]

システムログ情報を受信するサーバを指定しないものとみなされます。

11.2.2 syslog pri

[機能]

システムログ情報の出力対象プライオリティの設定

[入力形式]

syslog pri <mode>

[パラメタ]

<mode>

- プライオリティ
  システムログ情報を出力する対象となるプライオリティを、以下の中から指定します。複数指定する場合は、","(カンマ) で区切ります。

  error プライオリティLOG_ERROR を対象とする場合に指定します。

  warn プライオリティLOG_WARNING を対象とする場合に指定します。

  notice プライオリティLOG_NOTICE を対象とする場合に指定します。

  info プライオリティLOG_INFO を対象とする場合に指定します。

[説明]

システムログ情報を出力する対象となるプライオリティを指定します。

[未設定時]

何も指定しないものとみなされ、システムログ情報は収集されません。

11.2.3　syslog facility

[機能]

システムログ情報の出力対象ファシリティの設定

[入力形式]

syslog facility <num>

[パラメタ]

<num>

- ファシリティ
  システムログ情報の出力対象となるファシリティ(種別) を、0〜23 の 10 進数値で設定します。
  0 を指定するとカーネルメッセージのみ出力対象とします。
  23 を指定するとすべてのメッセージを出力対象とします。

[説明]

システムログ情報を出力する対象となるファシリティを指定します。

[未設定時]

0 を指定したものとみなされます。

```
syslog facility 0
```

11.2.4 syslog security

[機能]

システムログ情報の出力対象セキュリティの設定

[入力形式]

syslog security <securetype>

[パラメタ]

<securetype>

- セキュリティ対象
  セキュリティログ情報の出力対象を、以下の中から指定します。
  複数指定する場合は、","(カンマ) で区切ります。

  ipfilter IP filter モジュールを対象とする場合に指定します。

  nat NAT モジュールを対象とする場合に指定します。

  ppp PPP モジュールを対象とする場合に指定します。

  dhcp DHCP モジュールを対象とする場合に指定します。

  proxydns
  ProxyDNS モジュールを対象とする場合に指定します。

  none すべてのモジュールを対象外とする場合に指定します。

[説明]

システムログ情報を出力する対象となるセキュリティを指定します。

[未設定時]

すべてを指定したものとみなされます。

```
syslog security ipfilter,nat,ppp,dhcp,proxydns
```

11.2.5　syslog dupcut

[機能]

システムログ情報の重複メッセージ出力の設定

[入力形式]

syslog dupcut <cut>

[パラメタ]

<cut>

- yes
  直前に出力されたメッセージが重複した場合、出力しません。
- no
  重複チェックを行わず、すべてのメッセージを出力します。

[説明]

システムログにメッセージを出力する際、直前に出力したメッセージと重複した場合に出力するかどうかを指定します。

[未設定時]

重複チェックを行わないものとみなされます。

```
syslog dupcut no
```

11.3 自動時刻設定情報

11.3.1 time auto server

[機能]

時刻情報の提供サーバの設定

[入力形式]

time auto server <address> <protocol>

[パラメタ]

<address>

- IP アドレス
  時刻情報を提供しているサーバの IP アドレスを指定します。

<protocol>

使用するプロトコルを指定します。

- time
  TIME プロトコル (TCP) を使用する場合に指定します。
- sntp
  簡易 NTP プロトコル (UDP) を使用する場合に指定します。

[説明]

時刻提供サーバの情報を設定します。
“time auto server” の<address>で指定した時刻提供サーバから、<protocol>で指定したプロトコルを使用して、自動的に時刻を設定します。

[未設定時]

自動時刻設定を行わないものとみなされます。

11.3.2　time auto interval

[機能]

時刻情報の自動設定間隔の設定

[入力形式]

time auto interval <time>

[パラメタ]

<time>

時刻情報を設定する間隔を指定します。

- start
  電源投入時またはリセット時に一度だけ、時刻情報を設定する場合に指定します。
- 間隔
  時刻情報を設定する間隔を、0 秒～最大 10 日の範囲で指定します。単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。

[説明]

自動時刻を設定する間隔を設定します。

[未設定時]

時刻提供サーバを使用する場合のみ、電源投入時またはリセット時に一度だけ時刻情報設定するものとみなされます。

```
time auto interval start
```

11.3.3 time auto delete

[機能]

時刻情報の自動設定の削除

[入力形式]

time auto delete

[説明]

自動時刻設定の設定情報を削除します。

11.3.4　time zone

[機能]

時刻情報のタイムゾーンの設定

[入力形式]

time zone <offset>

[パラメタ]

<offset>

- 差分
  本装置が使用するタイムゾーンを指定します。
  GMT(グリニッジ標準時間) からの時差を指定します。日本で使用する場合は、0900 を指定してください。

[説明]

タイムゾーンを設定します。

[未設定時]

```
time zone 0
```

11.4 ProxyDNS 情報

11.4.1 proxydns domain

[機能]

プロキシ DNS の順引き動作条件の設定

[入力形式]

proxydns domain <count> <qtype> <qname> <address> / <mask> reject (転送要求の破棄)
proxydns domain <count> <qtype> <qname> <address> / <mask> static <ipaddress> (固定 DNS サーバ指定)
proxydns domain <count> <qtype> <qname> <address> / <mask> to <remote_number> (相手ネットワーク指定)

[パラメタ]

<count>

- 転送先定義番号
  転送先定義番号として、0〜31 の 10 進数値を指定します。
  指定した値は、設定完了時に順方向にソートされてリナンバリングされます。また、指定した定義番号と同じ値を持つ転送先定義番号が存在する場合は、既存定義の前に挿入されます。

<qtype>

- 問い合わせタイプ番号
  1〜11、または 13〜65535 の 10 進数値を指定します。
  以下に、問い合わせタイプの一部分を示します。

名称	番号	説 明
A	1	ホスト・アドレス
NS	2	ドメインに対して認証されたネーム・サーバ
CNAME	5	別名（Alias 名、ドメイン名）
SOA	6	ゾーン管理開始
PTR	12	ドメイン名空間のほかの部分へのポインタ
HINFO	13	ホストが使用する CPU と OS
MX	15	ドメインに対するメール交換
SRV	33	サービス

- any
  PTR(12) を除くすべてのタイプを対象する場合に指定します。

<qname>

- ホスト名
  条件となるホスト名を、80 文字以内で指定します。
  ホスト名には、以下のワイルドカードを使用できます。
  - *(アスタリスク)
    0 文字以上の任意の文字列とみなされます。
  - ?(クェスチョンマーク)
    任意の一文字とみなされます。

以下に、ワイルドカードを使用したホスト名の記述例および一致例を示します。

www.*.com

以下のどの文字列とも一致するとみなされます。

・www.testa.com

・www.test1.test.com

test　以下のどの文字列とも一致するとみなされます。

・www.test.com

・test.com

・test.co.jp

www.test?.com

以下のどの文字列とも一致するとみなされます。

・www.test1.com

・www.test2.com

・www.testA.com

なお、ホスト名をチェックするときに、大文字と小文字の区別はされません。

<address>/<mask>

対象となる送信元 IP アドレス、マスクビット数を指定します。

- 送信元 IP アドレス/マスクビット数 (またはマスク値)
  対象となる送信元 IP アドレスとマスクビット数の組み合わせを指定します。マスク値は、最上位ビットから 1 で連続した値にしてください。
- any
  すべてのアドレスを対象とする場合に指定します。
  0.0.0.0/0(0.0.0.0/0.0.0.0) を指定するのと同じ意味になります。

<ipaddress>

- DNS サーバ IP アドレス
  要求を転送する DNS サーバの IP アドレスを指定します。

<remote_number>

- 転送先相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。

[説明]

プロキシ DNS の順引き動作条件を設定します。
各コマンドについて説明します。

転送要求の破棄

proxydns domain <count> <qtype> <qname> <address>/<mask> reject

指定した DNS 要求の転送を無効にするフィルタを設定します。

<qname>で指定するホスト名は、DNS データベースに登録されていても、そのホスト (群) へのアクセスを制限する場合に使用します。条件と一致した場合は破棄されます。

固定 DNS サーバの指定

proxydns domain <count> <qtype> <qname> <address>/<mask> static <ipaddress>

指定した DNS 要求の転送先 IP アドレスを指定します。

以下の場合に有効です。

- 専用線に接続する場合
- LAN 側に DNS サーバが存在する場合
- リモート側の DNS サーバを固定にする場合

転送先への経路は、IP ルーティングに従って決められます。

相手ネットワークの指定

proxydns domain <count> <qtype> <qname> <address>/<mask> to <remote_number>

リモート側の回線の DNS サーバを使用します。

リモート定義でマルチルーティングを定義している場合は、その設定に従います。回線切断中は、アクセスポイントの接続優先順位に従います。

[未設定時]

プロキシ DNS の順引き動作条件を設定しないものとみなされます。

11.4.2　proxydns domain move

[機能]

プロキシ DNS の順引き動作条件の順序の変更

[入力形式]

proxydns domain move <count> <new_count>

[パラメタ]

<count>

- 変更前転送先定義番号
  順序を変更する転送先定義番号を指定します。

<new_count>

- 新しい転送先定義番号
  <count>に対して、新しい順序を指定します。
  すでにこの定義番号を持つ定義が存在する場合には、その定義の前に挿入されます。

[説明]

プロキシ DNS の順引き動作条件の順序を変更します。
すでに存在する転送先定義番号と同じ番号を指定した場合には、指定した定義の前に挿入されます。

11.4.3 proxydns domain delete

[機能]

プロキシ DNS の順引き動作条件の削除

[入力形式]

proxydns domain delete <count>

[パラメタ]

<count>

削除する転送先定義を指定します。

- 転送先定義番号
  削除する転送先定義番号を指定します。
- all
  すべての転送先定義番号を削除する場合に指定します。

[説明]

プロキシ DNS の順引き動作条件を削除します。

11.4.4　proxydns address

[機能]

プロキシ DNS の逆引き動作条件の設定

[入力形式]

proxydns address <count> <address>/<mask> reject (転送要求の破棄)
proxydns address <count> <address>/<mask> static <ipaddress> (固定 DNS サーバ指定)
proxydns address <count> <address>/<mask> to <remote_number> (相手ネットワーク指定)

[パラメタ]

<count>

- 転送先定義番号
  転送先定義番号として、0〜31 の 10 進数値を指定します。
  指定した値は、設定完了時に順方向にソートされてリナンバリングされます。また、指定した定義番号と同じ値を持つ転送先定義番号が存在する場合は、既存定義の前に挿入されます。

<address>/<mask>

逆引き対象 IP アドレス、マスクビット数を指定します。

- 逆引き対象 IP アドレス/マスクビット数 (またはマスク値)
  逆引き対象 IP アドレスとマスクビット数の組み合わせを指定します。
  マスク値は、最上位ビットから 1 で連続した値にしてください。
- any4
  IPv4 アドレスの逆引きのすべてを対象とする場合に指定します。
- any6
  IPv6 アドレスの逆引きのすべてを対象とする場合に指定します。
- any
  すべてのアドレスの逆引きを対象とする場合に指定します。

<ipaddress>

- DNS サーバ IP アドレス
  要求を転送する DNS サーバの IP アドレスを指定します。

<remote_number>

- 転送先相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。

[説明]

プロキシ DNS の逆引き動作条件を設定します。
各コマンドについて説明します。

転送要求の破棄

proxydns address <count> <address>/<mask> reject
指定した DNS 要求の転送を無効にするフィルタを設定します。
<qname>で指定するホスト名は、DNS データベースに登録されていても、そのホスト (群) へのアクセスを制限する場合に使用します。条件と一致した場合は破棄されます。

固定 DNS サーバの指定

proxydns address <count> <address>/<mask> static <ipaddress>

指定した DNS 要求の転送先 IP アドレスを指定します。

以下の場合に有効です。

- 専用線に接続する場合
- LAN 側に DNS サーバが存在する場合
- リモート側の DNS サーバを固定にする場合

転送先への経路は、IP ルーティングに従って決められます。

相手ネットワークの指定

proxydns address <count> <address>/<mask> to <remote_number>

リモート側の回線の DNS サーバを使用します。

リモート定義でマルチルーティングを定義している場合は、その設定に従います。回線切断中は、アクセスポイントの接続優先順位に従います。

[未設定時]

プロキシ DNS の逆引き動作条件を設定しないものとみなされます。

11.4.5　proxydns address move

[機能]

プロキシ DNS の逆引き動作条件の順序の変更

[入力形式]

proxydns address move <count> <new_count>

[パラメタ]

<count>

- 変更前転送先定義番号
  順序を変更する転送先定義番号を指定します。

<new_count>

- 新しい転送先定義番号
  <count>に対して、新しい順序を指定します。
  すでにこの定義番号を持つ定義が存在する場合には、その定義の前に挿入されます。

[説明]

プロキシ DNS の逆引き動作条件の順序を変更します。
すでに存在する転送先定義番号と同じ番号を指定した場合には、指定した定義の前に挿入されます。

11.4.6 proxydns address delete

[機能]

プロキシ DNS の逆引き動作条件の削除

[入力形式]

proxydns address delete <count>

[パラメタ]

<count>

削除する転送先定義を指定します。

- 転送先定義番号
  削除する転送先定義番号を指定します。
- all
  すべての転送先定義番号を削除する場合に指定します。

[説明]

プロキシ DNS の逆引き動作条件を削除します。

11.4.7　proxydns unicode

[機能]

プロキシ DNS の問い合わせパケットの透過の可否の設定

[入力形式]

proxydns unicode <action>

[パラメタ]

<action>

パケットを透過するかどうかを指定します。

- pass
  該当するパケットを透過する場合に指定します。
- reject
  該当するパケットを破棄する場合に指定します。

[説明]

プロキシ DNS の問い合わせ名 (QNAME) に非表示文字が含まれる場合に、その問い合わせのパケットを透過するかどうかを設定します。

[未設定時]

該当パケットを破棄するものとみなされます。

```
proxydns unicode reject
```

11.5 ホストデータベース情報

11.5.1 host name

[機能]

ホストデータベース情報のホスト名の設定

[入力形式]

host <number> name <name>

[パラメタ]

<number>

- 定義番号

  ホストデータベース情報の定義番号を、0〜63 の 10 進数値で指定します。

<name>

- ホスト名

  ホスト名を、英数字、"-"(ハイフン)、"."(ピリオド) で構成される 80 文字以内の ASCII 文字列で指定します。

[説明]

本装置配下に接続されたホストのホスト名をホストデータベースに設定します。
本コマンドは、簡易 DNS サーバ機能、DHCP スタティック機能、リモートパワーオン機能から利用されます。
以下に、各機能とパラメタの関係を示します。

パラメタ / 機能	name	ip_address	mac_address	wakeup_id	rpon
簡易DNSサーバ	○	○	—	—	—
DHCPスタティック	—	○	○	—	—
リモートパワーオン (ISDN接続先から)	—	—	○	○	—
リモートパワーオン (手動/schedule)	—	—	○	—	○

○:有効　—:無効

[未設定時]

ホストデータベースを設定しないものとみなされます。

11.5.2　host ip address

[機能]

ホストデータベース情報の IP アドレスの設定

[入力形式]

host <number> ip address <ip_address>

[パラメタ]

<number>

- 定義番号

  ホストデータベース情報の定義番号を、0～63 の 10 進数値で指定します。

<ip_address>

- IP アドレス

  ホストの IP アドレスを指定します。

[説明]

本装置配下に接続されたホストの IP アドレスをホストデータベースに設定します。
本コマンドは、簡易 DNS サーバ機能、DHCP スタティック機能、リモートパワーオン機能から利用されます。
以下に、各機能とパラメタの関係を示します。

パラメタ / 機能	name	ip_address	mac_address	wakeup_id	rpon
簡易DNSサーバ	○	○	―	―	―
DHCPスタティック	―	○	○	―	―
リモートパワーオン (ISDN接続先から)	―	―	○	○	―
リモートパワーオン (手動/schedule)	―	―	○	―	○

○:有効　―:無効

[未設定時]

ホストデータベースを設定しないものとみなされます。

11.5.3 host mac

[機能]

ホストデータベース情報の MAC アドレスの設定

[入力形式]

host <number> mac <mac_address>

[パラメタ]

<number>

- 定義番号

  ホストデータベース情報の定義番号を、0～63 の 10 進数値で指定します。

<mac_address>

- MAC アドレス

  ホストの MAC アドレスを、xx:xx:xx:xx:xx:xx(xx は 2 桁の 16 進数値) の形式で指定します。

[説明]

本装置配下に接続されたホストの MAC アドレスをホストデータベースに設定します。
本コマンドは、簡易 DNS サーバ機能、DHCP スタティック機能、リモートパワーオン機能から利用されます。
以下に、各機能とパラメタの関係を示します。

パラメタ / 機能	name	ip_address	mac_address	wakeup_id	rpon
簡易DNSサーバ	○	○	―	―	―
DHCPスタティック	―	○	○	―	―
リモートパワーオン (ISDN接続先から)	―	―	○	○	―
リモートパワーオン (手動/schedule)	―	―	○	―	○

○:有効　―:無効

[未設定時]

ホストデータベースを設定しないものとみなされます。

11.5.4　host wakeid

[機能]

ホストデータベース情報の Wakeup-ID の設定

[入力形式]

host <number> wakeid <wakeup_id>

[パラメタ]

<number>

- 定義番号

  ホストデータベース情報の定義番号を、0～63 の 10 進数値で指定します。

<wakeup_id>

- Wakeup-ID

  Wakeup-ID を、0x21,0x23～0x7e の 19 文字以内 ASCII 文字列で指定します。

[説明]

本装置配下に接続されたホストの Wakeup-ID をホストデータベースに設定します。
本コマンドは、簡易 DNS サーバ機能、DHCP スタティック機能、リモートパワーオン機能から利用されます。
以下に、各機能とパラメタの関係を示します。

パラメタ / 機能	name	ip_address	mac_address	wakeup_id	rpon
簡易DNSサーバ	○	○	―	―	―
DHCPスタティック	―	○	○	―	―
リモートパワーオン (ISDN接続先から)	―	―	○	○	―
リモートパワーオン (手動/schedule)	―	―	○	―	○

○:有効　―:無効

[未設定時]

ホストデータベースを設定しないものとみなされます。

11.5.5 host rpon

[機能]

ホストデータベース情報のリモートパワーオン対象の設定

[入力形式]

host <number> rpon <rpon>

[パラメタ]

<number>

- 定義番号
  ホストデータベース情報の定義番号を、0～63 の 10 進数値で指定します。

<rpon>

リモートパワーオンの対象にするかどうかを設定します。

- off
  リモートパワーオンの対象にしません。

[説明]

本装置配下に接続されたホストのリモートパワーオン情報をホストデータベースに設定します。
本コマンドは、簡易 DNS サーバ機能、DHCP スタティック機能、リモートパワーオン機能から利用されます。
以下に、各機能とパラメタの関係を示します。

パラメタ / 機能	name	ip_address	mac_address	wakeup_id	rpon
簡易DNSサーバ	○	○	―	―	―
DHCPスタティック	―	○	○	―	―
リモートパワーオン (ISDN接続先から)	―	―	○	○	―
リモートパワーオン (手動/schedule)	―	―	○	―	○

○:有効　―:無効

[未設定時]

リモートパワーオンの対象にするものとみなされます。

11.5.6　host delete

[機能]

ホストデータベース情報の削除

[入力形式]

host delete <number>

[パラメタ]

<number>

- 定義番号
  削除するホストデータベース情報の定義番号を指定します。
- all
  すべてのホストデータベース情報を削除する場合に指定します。

[説明]

ホストデータベースの情報を削除します。

11.6　パスワード 情報

11.6.1　password set

[機能]

ログオンパスワード の設定

[入力形式]

password set <pass> [encrypted] [<mode>]

[パラメタ]

<pass>

- パスワード
  パスワード の文字列を、0x21,0x23～0x7e の 16 文字以内の ASCII 文字で指定します。
- 暗号化されたパスワード
  show コマンド で表示される暗号化されたパスワード を encrypted と共に指定します。
  show コマンド で表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化パスワード 指定
  <pass>に暗号化されたパスワード を指定する場合に指定します。

<mode>

- パスワード 問い合わせモード
  パスワード の問い合わせモード を、0～7 の 8 進数値で指定します。
  <mode>は、以下の<mode>のいくつかの論理和をとったものとします。
  省略した場合は、0 を指定したものとみなされます。
  WWW ブラウザを使用して本装置の操作、表示、保守を行う場合に、処理メニュー単位にパスワード を問い合わせるかどうかを設定できます。

  4　「操作メニュー」でパスワード を問い合わせます。
  2　「表示メニュー」でパスワード を問い合わせます。
  1　「保守メニュー」でパスワード を問い合わせます。

[説明]

ログオンパスワード を設定します。
パスワード は、本コマンド で設定した直後に有効となります。

[注意]

show コマンド では、暗号化されたパスワード が encrypted と共に表示されます。

[未設定時]

パスワード は設定されていません。

11.6.2　password delete

[機能]

ログオンパスワードの削除

[入力形式]

password delete

[説明]

ログオンパスワードを削除します。

11.7　スケジュール情報

11.7.1　schedule at

[機能]

システムスケジュールの日時指定コマンドの設定

[入力形式]

schedule <number> at <day> <time> <command>

[パラメタ]

<number>

スケジュール定義を指定します。

- スケジュール定義番号
  スケジュール定義番号を、0～15 の 10 進数値で指定します。
- any
  スケジュール定義番号を省略する場合に指定します。

<day>

- 日
  スケジュールの実行日または開始日を、1～31 の 10 進数値で指定します。
- 曜日
  スケジュールの実行曜日または開始曜日を、以下の中から指定します。

sun	日曜日
mon	月曜日
tue	火曜日
wed	水曜日
thu	木曜日
fri	金曜日
sat	土曜日

  複数の曜日を指定する場合は、","(カンマ) で区切って指定します。
- any
  スケジュールの実行日または開始日を毎日とする場合に指定します。
  電源投入時または再起動時は、本パラメタを指定してください。

<time>

- 実行時間
  実行する時、分を、0～9 の 4 桁の 10 進数値で指定します (例: 0635 = 午前 6 時 35 分、2330 = 午後 11 時 30 分)。
- pwon
  電源投入時に実行する場合に指定します。
- rset
  システム再起動時、または電源投入時に実行する場合に指定します。

<command>

実行するコマンド文字列を指定します。

- isdnstat -dramc
  課金情報をクリアする場合に指定します。
- disconnect all
  強制切断する場合に指定します。
- mstat all
  統計情報をシスログメッセージとして送信する場合に指定します。
  以下のコマンド実行結果が統計情報として送信されます。
  - isdnstat -dra
  - stins
  - stlan
- rpon all
  リモートパワーオンを実行する場合に指定します。
- power low
  スタンバイモードへ移行する場合に指定します。
- power high
  スタンバイモードを解除する場合に指定します。
- absence on
  留守モードへ移行する場合に指定します。
- absence off
  留守モードを解除する場合に指定します。

[説明]

システムスケジュールを設定します。
このスケジュールに従って、指定した時刻にコマンドを実行します。

[未設定時]

スケジュール情報を設定しないものとみなされます。

11.7.2 schedule in

[機能]

システムスケジュールの期間指定動作の設定

[入力形式]

schedule <number> in <day> <time> <action>

[パラメタ]

<number>

スケジュール定義を指定します。

- スケジュール定義番号
  スケジュール定義番号を、0～15 の 10 進数値で指定します。
- any
  スケジュール定義番号を省略する場合に指定します。

<day>

- 日
  スケジュールの実行日または開始日を、1～31 の 10 進数値で指定します。
- 曜日
  スケジュールの実行曜日または開始曜日を、以下の中から指定します。

sun	日曜日
mon	月曜日
tue	火曜日
wed	水曜日
thu	木曜日
fri	金曜日
sat	土曜日

  複数の曜日を指定する場合は、","(カンマ) で区切って指定します。
- any
  スケジュールの実行日または開始日を毎日とする場合に指定します。
  電源投入時または再起動時は、本パラメタを指定してください。

<time>

- 開始時刻～終了時刻
  開始時刻～終了時刻を、0～9 の 4 桁の 10 進数値で指定します。開始時刻と終了時刻の間は、"-"(ハイフン) でつなぎます (例: 0900-1700 = 午前 9 時から午後 5 時まで、2300-0800 = 午後 11 時から翌午前 8 時まで)。

<action>

動作を指定します。

- diallock
  <time>で指定した時刻の間、自動発信を抑止します。
- dialreject
  <time>で指定した時刻の間、自動着信を抑止します。
- timerctl
  <time>で指定した時間の間、無通信監視タイマによる切断を行いません。ただし、相手情報の接続保持情報が設定が無効 (off) の場合は対象になりません。

[説明]

システムスケジュールを設定します。
このスケジュールに従って、指定した時刻の間、ある状態を維持することができます。

[未設定時]

スケジュール情報を設定しないものとみなされます。

11.7.3 schedule syslog

[機能]

システムスケジュールのシステムログ出力可否の設定

[入力形式]

schedule <number> syslog <syslog>

[パラメタ]

<number>

スケジュール定義を指定します。

- スケジュール定義番号
  スケジュール定義番号を、0～15 の 10 進数値で指定します。
- any
  スケジュール定義番号を省略する場合に指定します。

<syslog>

- yes
  コマンド実行時の出力をシステムログで行う場合に指定します。
- no
  コマンド実行時の出力をシステムログで行わない場合に指定します。

[説明]

スケジュールによって起動されたコマンドが出力するメッセージを、システムログに出力するかどうかを指定します。
スケジュールで起動するコマンドが指定されている場合にのみ有効です。

[未設定時]

コマンド実行時の出力をシステムログに出力しないものとみなされます。

```
schedule <number> syslog no
```

11.7.4　schedule delete

[機能]

システムスケジュールの削除

[入力形式]

schedule delete <number>

[パラメタ]

<number>

削除するスケジュール定義を指定します。

- スケジュール定義番号
  削除するスケジュール定義番号を指定します。
- all
  すべてのスケジュール定義を削除する場合に指定します。

[説明]

システムスケジュールを削除します。

11.8　電話番号変更予約情報

11.8.1　dnconvinfo date

[機能]

電話番号変更予約の日時の設定

[入力形式]

dnconvinfo <index> date <date>

[パラメタ]

<index>

- 登録番号
  電話番号変更予約情報の登録番号を、0～3 の 10 進数値で指定します。

<date>

- 変更日時
  変更日時を、yymmddHHMM の形式で指定します。

yy	西暦の下 2 桁を指定します。西暦 2036 年まで指定できます。
mm	月を、1～12 の 10 進数値で指定します。
dd	日付を、1～31 の 10 進数値で指定します。
HH	時間を、0～23 の 10 進数値で指定します。
MM	分を、0～59 の 10 進数値で指定します。

[説明]

すべての構成定義情報の電話番号を一括変更する場合に必要となる、電話番号変更日時を設定します。
変更処理は、以下の 2 つの方法によって行われます。

- 時刻指定によって、スケジュール機能から自動的に実施します。
  なお、スケジュール機能によって実施した場合は、定義情報が保存され、システムがリセット されます。
- 時刻指定によらずに、コマンド で実施します。

[注意]

以下に、スケジュール機能によって電話番号変更を実施する場合の注意事項を示します。

- 装置の時刻を正しく設定してください。
- 実施時刻に、装置の電源を投入しておいてください。

[例]

以下に、構成定義情報に定義されている電話番号 123456789 を、2008 年 1 月 1 日午前 2 時にすべて 999999999 へ変更する場合の設定例を示します。

```
# dnconvinfo 0 date 0801010200
# dnconvinfo 0 dial 0 123456789 99999999
# show dnconvinfo
0 date 0801010200
0 dial 0 123456789 99999999
#
```

[未設定時]

電話番号変更予約情報を設定しないものとみなされます。

11.8.2 dnconvinfo dial

[機能]

電話番号変更予約の電話番号の設定

[入力形式]

dnconvinfo <index> dial <count> <src_number> <dst_number>

[パラメタ]

<index>

- 登録番号
  電話番号変更予約情報の登録番号を、0～3 の 10 進数値で指定します。

<count>

- 電話番号情報定義番号
  電話番号情報の定義番号を、0～3 の 10 進数値で指定します。

<src_number>

- 変更前電話番号
  変更対象の電話番号を、0～9 の数字と、*、#、-、(、)、\の文字で構成される 32 桁以内の ASCII 文字列で指定します。

<dst_number>

- 変更後電話番号
  変更後の電話番号を、0～9 の数字と、*、#、-、(、)、\の文字で構成される 32 桁以内の ASCII 文字列で指定します。

[説明]

すべての構成定義情報の電話番号を一括変更する場合に必要となる、変更電話番号を設定します。
変更処理は、以下の 2 つの方法によって行われます。

- 時刻指定によって、スケジュール機能から自動的に実施します。
  なお、スケジュール機能によって実施した場合は、定義情報が保存され、システムがリセットされます。
- 時刻指定によらずに、コマンドで実施します。

[注意]

以下に、スケジュール機能によって電話番号変更を実施する場合の注意事項を示します。

- 装置の時刻を正しく設定してください。
- 実施時刻に、装置の電源を投入しておいてください。

[例]

以下に、構成定義情報に定義されている電話番号 123456789 を、2008 年 1 月 1 日午前 2 時にすべて 999999999 へ変更する場合の設定例を示します。

```
# dnconvinfo 0 date 0801010200
# dnconvinfo 0 dial 0 123456789 99999999
# show dnconvinfo
0 date 0801010200
0 dial 0 123456789 99999999
#
```

[未設定時]

電話番号変更予約情報を設定しないものとみなされます。

11.8.3 dnconvinfo dial delete

[機能]

電話番号変更予約の電話番号の削除

[入力形式]

dnconvinfo <index> dial delete <count>

[パラメタ]

<index>

- 登録番号
  電話番号変更予約情報の登録番号を、0～3 の 10 進数値で指定します。

<count>

- 電話番号情報定義番号
  削除する電話番号情報の定義番号を指定します。
- all
  すべての電話番号情報を削除する場合に指定します。

[説明]

変更電話番号を削除します。

11.8.4　dnconvinfo delete

[機能]

電話番号変更予約の削除

[入力形式]

dnconvinfo delete <index>

[パラメタ]

<index>

- 登録番号
  削除する電話番号変更予約情報の登録番号を指定します。
- all
  すべての電話番号変更予約情報を削除する場合に指定します。

[説明]

電話番号変更予約情報を削除します。

11.9 ファームウェア更新情報

11.9.1 updateinfo

[機能]

ファームウェア更新情報の設定

[入力形式]

updateinfo <host> <user> <pass> <pathname>

[パラメタ]

<host>

- ホスト名
  更新するファームウェアが存在するホスト名を、0x21,0x23～0x7e の 128 文字以内の ASCII 文字列を指定します。
  ホスト名を指定した場合は、ルータ装置が DNS サーバを使用可能な状態でなければなりません。
- IP アドレス
  更新するファームウェアが存在するホストの IP アドレスを指定します。
  ルータ装置が DNS サーバを利用できない場合に、IP アドレスを直接指定してください。

<user>

- ユーザ名
  ファームウェアを更新するときに使用する ftp ユーザ名を、0x21,0x23～0x7e の 16 文字以内の ASCII 文字列で指定します。

<pass>

- パスワード
  ファームウェア更新のときに使用する ftp パスワードを、0x21,0x23～0x7e の 32 文字以内の ASCII 文字列で指定します。anonymous FTP サーバの場合は、管理者のメールアドレスを指定します。

<pathname>

- パス名
  更新するファームウェアが存在する ftp サーバ上のパス名を、0x21,0x23～0x7e の 80 文字以内の ASCII 文字列で指定します。

[説明]

ファームウェアを更新するための情報を設定します。
“14.1.6 update” で ftp サーバ上のファームウェアを取得する場合は、必ず本コマンドを実行してください。

[未設定時]

ファームウェア更新情報を設定しないものとみなされます。

11.9.2　updateinfo delete

[機能]

ファームウェア更新情報の削除

[入力形式]

updateinfo delete

[パラメタ]

なし

[説明]

ファームウェアを更新するための情報を削除します。

11.10　オンラインサポート 情報

11.10.1　rcmdinfo callin

[機能]

オンラインサポート接続要求の受付可否の設定

[入力形式]

rcmdinfo callin <mode>

[パラメタ]

<mode>

- accept
  オンラインサポート接続要求を受け付けます。
- reject
  オンラインサポート接続要求を拒否します。

[説明]

オンラインサポート接続要求を受け付けるかどうかを設定します。

[注意]

着信時に通知される相手電話番号と着サブアド レスが、rcmdinfo auth <number> [<subaddress>] の設定内容と一致しない場合、着信を拒否します。

[未設定時]

オンラインサポート接続要求を受け付けるものとみなされます。

```
rcmdinfo callin accept
```

11.10.2　rcmdinfo auth

[機能]

オンラインサポート接続の認証情報の設定

[入力形式]

rcmdinfo auth <number> [<subadderss>]

[パラメタ]

<number>

- 相手電話番号
  着信時にチェックする相手電話番号を、0～9 の数字と、*、#、-、(、)、\の文字で構成される 32 桁以内の ASCII 文字列で指定します。
- any
  着信時に相手電話番号をチェックしない場合に指定します。
  なお、<subaddress>を指定する場合は、<subaddress>だけをチェックします。

<subaddress>

- 着サブアドレス
  着信時にチェックする着サブアドレスを、0x21,0x23～0x7e の文字で構成される 19 桁以内の ASCII 文字列で指定します。

[説明]

オンラインサポート接続の着信時にチェックする相手電話番号と着サブアドレスを設定します。着信時に通知される相手電話番号と着サブアドレスが本設定と一致しない場合、着信を拒否します。

[注意]

<number>を any とし<subaddress>を省略した場合には、<subaddress>に本装置の MAC アドレスが設定されているものとみなされます。
初期状態の本装置に対してオンラインサポート接続する場合には、着サブアドレスに本装置の MAC アドレスを 12 桁の 16 進数 (半角小文字の英数字) で指定します。
rcmdinfo callin reject と設定されている場合、本設定にかかわらずオンラインサポート接続の着信を拒否します。

[未設定時]

着信時に相手電話番号をチェックしないものとみなされます。
<subaddress>には本装置の MAC アドレスが設定されているものとみなされます。

```
rcmdinfo auth any
```

11.11　マルチ TA 情報

11.11.1　mta service

[機能]

マルチ TA 機能の使用有無の設定

[入力形式]

mta service <mode>

[パラメタ]

<mode>

- 0
  マルチ TA 機能を使用しません。
- 1
  クライアントの同時アクセス数 1 で使用します。
- 2
  クライアントの同時アクセス数 2 で使用します。

[説明]

マルチ TA 機能の使用有無を設定します。

[注意]

マルチ TA 機能は、Windows Vista®では使用できません。

[未設定時]

マルチ TA 機能を使用しないものとみなされます。

```
mta service 0
```

11.11.2　mta mask

[機能]

マルチ TA 機能の利用可能ホストの設定

[入力形式]

mta mask <addr> / <mask>

[パラメタ]

<addr>/<mask>

- 許可 IP アドレス / マスクビット数 (またはマスク値)
  マルチ TA 機能の利用を許可するホストの IP アドレス / マスクビット数 (またはマスク値) を指定します。
  マスク値は、最上位ビットから 1 で連続した値にしてください。
- any
  すべてのホスト (IP アドレス) から使用可能とする場合に指定します。
  0.0.0.0 / 0(0.0.0.0 / 0.0.0.0) を指定するのと同じ意味になります。

[説明]

マルチ TA 機能の利用を許可するホストの IP アドレス範囲を設定します。

[未設定時]

すべてのホストからの利用を許可するものとみなされます。

```
mta mask any
```

11.11.3 mta timer

[機能]

マルチ TA 機能の強制切断タイマの設定

[入力形式]

mta timer <time>

[パラメタ]

<time>

- 強制切断タイマ
  異常課金を防止するための強制切断タイマを、0 秒～86400 秒 (1 日) の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。
  0 を指定した場合は、切断されません。

[説明]

マルチ TA 通信時の強制切断タイマの値を設定します。

[未設定時]

強制切断を行わないものとみなされます。

```
mta timer 0d
```

11.12　留守モード 情報

11.12.1　absenceinfo

[機能]

留守モード 情報の設定

[入力形式]

absenceinfo <action,...>

[パラメタ]

<action>

留守モード 時の動作を、以下の中から指定します。複数指定する場合は、","(カンマ) で区切ります。ただし、deflection と pseudo は同時に設定できません。

- power
  留守中は、スタンバイモード で動作します。
- check
  留守モード を解除するときにメールチェックを行います。
- tel
  留守中は、TEL メールを送信します。
- trans
  留守中は、メールを転送します。
- list
  留守中は、メールの一覧を送信します。
- deflection
  留守中は、着信転送を行います。
- pseudo
  留守中は、疑似着信転送を行います。
- homeout
  留守中は、アナログの留守確認機能を使用します。

[説明]

留守モード 時の動作を設定します。

[未設定時]

留守モード 情報を設定しないものとみなされます。

11.12.2 absenceinfo delete

[機能]

留守モード情報の削除

[入力形式]

absenceinfo delete

[説明]

留守モード情報の設定を削除します。

11.13　その他

11.13.1　addact

[機能]

コマンド 実行予約の設定

[入力形式]

addact <index> <date> <command>

[パラメタ]

<index>

- 登録番号
  コマンド 実行予約情報の登録番号を指定します。必ず 0 を指定してください。

<date>

- 実行日時
  コマンド 実行日時を、yymmddHHMM の形式で指定します。

yy	西暦の下 2 桁を指定します。西暦 2036 年まで指定できます。
mm	月を、1〜12 の 10 進数値で指定します。
dd	日付を、1〜31 の 10 進数値で指定します。
HH	時間を、0〜23 の 10 進数値で指定します。
MM	分を、0〜59 の 10 進数値で指定します。

<command>

実行するコマンド 文字列を指定します。

- reset config1
  構成定義 1 に切り替えて再起動する場合に指定します。
- reset config2
  構成定義 2 に切り替えて再起動する場合に指定します。

上記以外のコマンド を指定した場合の動作は保証されません。

[説明]

コマンド 実行予約を設定します。

[注意]

以下に、スケジュール機能によってコマンド を実行する場合の注意事項を示します。

- 装置の時刻を正しく設定してください。
- 実施時刻に、装置の電源を投入しておいてください。

[例]

以下に、2008 年 1 月 1 日 午前 2 時 に構成定義 2 に切り替えて再起動する場合の設定例を示します。

```
# addact 0 0801010200 reset config2
# show addact
0 0801010200 reset config2
#
```

[未設定時]

コマンド の実行予約を行わないものとみなされます。

11.13.2　addact delete

[機能]

コマンド実行予約の削除

[入力形式]

addact delete <index>

[パラメタ]

<index>

削除するコマンド実行予約の登録番号を指定します。

- 登録番号
  削除するコマンド実行予約情報の登録番号を指定します。
- all
  すべての登録番号を削除する場合に指定します。

[説明]

コマンド実行予約を削除します。

11.13.3 consoleinfo

[機能]

シリアルコンソール接続サービスの設定

[入力形式]

consoleinfo autologout <time>

[パラメタ]

<time>

- 強制ログアウト時間

  シリアルコンソールでログインしたままコマンド実行が行われない状態が続いたときに強制ログアウトさせる時間を、0 秒～86400 秒 (1 日) の範囲で指定します。

  単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。

  0 秒を指定した場合には、強制ログアウトしません。

[説明]

シリアルコンソールでログインしたまま<time>で指定した時間内にコマンド実行されなかった場合、強制的にログアウトさせるように設定します。

[未設定時]

強制ログアウトさせないものとみなされます。

```
consoleinfo autologout 0s
```

11.13.4　telnetinfo

[機能]

TELNET 接続サービスの設定

[入力形式]

telnetinfo autologout <time>

[パラメタ]

<time>

- 自動切断時間

  telnet 接続したクライアントからコマンド入出力が行われない状態で自動切断するまでの時間を、0 秒～86400 秒 (1 日) の範囲で指定します。単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。

[説明]

TELNET コネクションの入出力がない場合にコネクションを切断するまでの時間を設定します。

[未設定時]

TELNET コネクションの入出力の監視を行わないものとみなされます。

```
telnetinfo autologout 0s
```

第 12 章　E メールエージェント情報の設定

12.1　メールチェック情報

12.1.1　email delete

[機能]

E メールエージェントのユーザ情報の削除

[入力形式]

email delete <count>

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。
- all
  すべてのユーザ定義番号を削除の対象とします。

[説明]

E メールエージェントのユーザ情報を削除します。

12.1.2　email use

[機能]

E メールエージェントのユーザ情報の有効／無効の設定

[入力形式]

email [<count>] use <mode>

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<mode>

- on
  ユーザ情報を有効にします。
- off
  ユーザ情報を無効にします。

[説明]

E メールエージェントのユーザ情報を有効とするかどうかを設定します。
無効に設定しても、E メールエージェントのユーザ情報は削除されません。

[未設定時]

E メールエージェントのユーザ情報は有効とみなされます。

```
email <count> use on
```

12.1.3 email check delete

[機能]

メールチェック関連情報の削除

[入力形式]

email [<count>] check delete

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

[説明]

メールチェック関連情報を削除します。

12.1.4　email check server

[機能]

メールチェック時のメールサーバの設定

[入力形式]

email [<count>] check server <host> [<port>]

[パラメタ]

<count>

- ユーザ定義番号

  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<host>

- メールサーバ名

  メールサーバ (POP サーバ) のホスト名を、0x21,0x23～0x7e の 80 文字以内の ASCII 文字列で指定します。

  ホスト名を指定した場合は、本装置が DNS サーバを使用可能な状態でなければなりません。

- メールサーバ IP アドレス

  メールサーバ (POP サーバ) のホストの IP アドレスを指定します。

<port>

- ポート番号

  メールサーバ (POP3 サーバ) のポート番号を、1～65535 の 10 進数値で指定します。

  省略した場合は、110 を指定したものとみなされます。

[説明]

メールチェック時のメールサーバ (POP3 サーバ) の設定を行います。

[未設定時]

メールサーバは未設定です。

12.1.5 email check server delete

[機能]

メールチェック時のメールサーバの削除

[入力形式]

email [<count>] check server delete

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

[説明]

メールチェック時のメールサーバ (POP3 サーバ) の設定を削除します。

12.1.6　email check type

[機能]

メールチェック認証方式の設定

[入力形式]

email [<count>] check type <type>

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<type>

- pop
  POP の認証方式で USER / PASS コマンドを使用します。
- apop
  POP の認証方式で APOP コマンドを使用します。

[説明]

メールチェックの認証方式の設定を行います。

[未設定時]

POP の認証方式に USER / PASS コマンドを使用するものとみなされます。

12.1.7 email check user

[機能]

メールチェック認証情報の設定

[入力形式]

email [<count>] check user <user> <pass> [encrypted]

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0〜9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<user>

- ユーザ名
  メールの受信に使用するユーザ名を、0x21,0x23〜0x7e の 32 文字以内の ASCII 文字列で指定します。

<pass>

- パスワード
  メールの受信に使用するパスワードを、0x21,0x23〜0x7e の 80 文字以内の ASCII 文字列で指定します。
- 暗号化されたパスワード
  show コマンドで表示される暗号化されたパスワードを encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化パスワード指定
  <pass>に暗号化されたパスワードを指定する場合に指定します。

[説明]

メールチェック情報の認証情報の設定を行います。

[注意]

show コマンドでは、暗号化されたパスワードが encrypted と共に表示されます。
show email [<count>] check user を実行すると、暗号化していないパスワードが表示されます。

[未設定時]

ユーザ名およびパスワードは未設定です。

12.1.8　email check user delete

[機能]

メールチェック認証情報の削除

[入力形式]

email [<count>] check user delete

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

[説明]

メールチェックの認証情報を削除します。

12.1.9 email check rcheck

[機能]

リモート メールチェック ID の設定

[入力形式]

email [<count>] check rcheck <rcheck>

[パラメタ]

<count>

- ユーザ定義番号

  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<rcheck>

- リモート メールチェック ID

  遠隔地からメールチェックを行うための識別コード (サブアド レス) を、0x21,0x23～0x7e の 19 桁以内の ASCII 文字列で指定します。

  "delete"を指定することはできません。

[説明]

リモート メールチェックで使用する識別コード (サブアド レス) を設定します。

[未設定時]

リモート メールチェック ID は未設定です。

12.1.10　email check rcheck delete

[機能]

リモート メールチェック ID の削除

[入力形式]

email [<count>] check rcheck delete

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

[説明]

リモート メールチェックで使用する識別コード (サブアド レス) の設定を削除します。

12.1.11 email check action mode

[機能]

メールチェック動作モード の設定

[入力形式]

email [<count>] check action mode <mode>

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<mode>

- time
  指定時刻にメールチェックを行います。
- interval
  一定間隔でメールチェックを行います。

[説明]

メールチェックの動作モード を設定します。

- time
  指定時刻にメールチェックを行う場合は、email check action time で実行時刻を設定します。
- interval
  一定間隔でメールチェックを行う場合は、email check action interval で実行間隔を設定します。

[未設定時]

指定時刻にメールチェックを行うものとみなされます。

```
email <count> check action time
```

12.1.12　email check action time

[機能]

メールチェック実行時刻の設定

[入力形式]

email [<count>] check action time <time_count> <day> <time>

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<time_count>

- 実行時刻定義番号
  メールチェック実行時刻の定義番号を、0～2 の 10 進数値で指定します。

<day>

- 曜日
  メールチェックを実行する曜日を、以下の中から指定します。

sun	日曜日
mon	月曜日
tue	火曜日
wed	水曜日
thu	木曜日
fri	金曜日
sat	土曜日

- any
  メールチェックの実行を毎日とする場合に指定します。

<time>

- 実行時刻
  実行する時、分を、0～9 の 4 桁の 10 進数値で指定します。
  (例: 0635 = 午前 6 時 35 分、2330 = 午後 11 時 30 分)

[説明]

メールチェックの実行時刻を設定します。
メールチェックの実行時刻は、3 個まで定義できます。

[未設定時]

メールチェックの実行時刻は未設定です。

12.1.13 email check action time delete

[機能]

メールチェック実行時刻の削除

[入力形式]

email [<count>] check action time delete <time_count>

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<time_count>

削除するメールチェック実行時刻を指定します。

- 削除する実行時刻定義番号
  削除する実行時刻定義番号を指定します。
- all
  すべての実行時刻の設定を削除する場合に指定します。

[説明]

メールチェックの実行時刻の設定を削除します。

12.1.14　email check action interval

[機能]

メールチェック実行間隔の設定

[入力形式]

email [<count>] check action interval <time>

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<time>

- 実行間隔
  メールチェック実行間隔を、18000 秒 (5 分)～2592000 秒 (30 日) の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。

[説明]

メールチェックの実行間隔を設定します。

[未設定時]

メールチェックの実行間隔は未設定です。

12.1.15 email check action interval delete

[機能]

メールチェック実行間隔の削除

[入力形式]

email [<count>] check action interval delete

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

[説明]

メールチェックの実行間隔の設定を削除します。

12.2　メール転送情報

12.2.1　email send delete

[機能]

メール転送／メール一覧送信関連情報の削除

[入力形式]

email [<count>] send delete

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

[説明]

メール転送／メール一覧関連情報を削除します。

12.2.2 email send use

[機能]

メール転送の使用有無の設定

[入力形式]

email [<count>] send use <mode>

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<mode>

- on
  メール転送します。
- off
  メール転送しません。

[説明]

メールを転送するかどうかを設定します。

[未設定時]

メールを転送しないものとみなされます。

```
email <count> send use off
```

12.2.3　email send server

[機能]

メール転送／メール一覧送信の送信サーバの設定

[入力形式]

email [<count>] send server <host> [<port>]

[パラメタ]

<count>

- ユーザ定義番号

  ユーザ定義番号を、0〜9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<host>

- メールサーバ名

  メール送信に使用するメールサーバ (SMTP サーバ) のホスト名を、0x21,0x23〜0x7e の 80 文字以内の ASCII 文字列で指定します。

  ホスト名を指定した場合は、本装置が DNS サーバを使用可能な状態でなければなりません。

- メールサーバ IP アドレス

  メール送信に使用するメールサーバ (SMPT サーバ) のホストの IP アドレスを指定します。

<port>

- ポート番号

  メールサーバ (SMTP サーバ) のポート番号を、1〜65535 の 10 進数値で指定します。省略した場合は、25 を指定したものとみなされます。

[説明]

メール転送／メール一覧送信で使用するメールサーバ (SMTP サーバ) を設定します。

[未設定時]

メール転送／メール一覧送信で使用するメールサーバ (SMTP サーバ) は未設定です。

12.2.4 email send server delete

[機能]

メール転送／メール一覧送信の送信サーバの削除

[入力形式]

email [<count>] send server delete

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

[説明]

メール転送／メール一覧送信で使用するメールサーバ (SMTP サーバ) の設定を削除します。

12.2.5　email send mailaddr

[機能]

メール転送／メール一覧送信の宛先メールアドレスの設定

[入力形式]

email [<count>] send mailaddr <mailaddr_count> <to>

[パラメタ]

<count>

- ユーザ定義番号

  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<mailaddr_count>

- 宛先メールアドレス定義番号

  宛先メールアドレス定義番号を、0～4 の 10 進数値で指定します。

<to>

- 宛先メールアドレス

  宛先メールアドレスを、0x21,0x23～0x7e の 80 文字以内の ASCII 文字列で指定します。

[説明]

メール転送／メール一覧送信で使用する宛先メールアドレスを設定します。
宛先メールアドレスは、4 個まで定義できます。

[未設定時]

メール転送／メール一覧送信の宛先メールアドレスは未設定です。

12.2.6 email send mailaddr delete

[機能]

メール転送／メール一覧送信の宛先メールアドレスの削除

[入力形式]

email [<count>] send mailaddr delete <mailaddr_count>

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<mailaddr_count>

- 削除する宛先メールアドレス定義番号
  削除する宛先メールアドレス定義番号を指定します。
- all
  すべての宛先メールアドレスを削除する場合に指定します。

[説明]

メール転送の宛先メールアドレスの設定を削除します。

12.2.7　email send from

[機能]

メール転送／メール一覧送信の差出人メールアドレスの設定

[入力形式]

email [<count>] send from <from>

[パラメタ]

<count>

- ユーザ定義番号

  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<from>

- 差出人メールアドレス

  メール転送時に変更する差出人メールアドレスを、0x21,0x23～0x7e の 80 文字以内の ASCII 文字列で指定します。

  "delete"を指定することはできません。

[説明]

メール転送／メール一覧送信で使用する差出人メールアドレスを変更する場合に設定します。本コマンドで設定されたメールアドレスを差出人メールアドレスとして、SMTP サーバにメールの送信を要求します。
差出人メールアドレスが未指定の場合は、メールチェック情報のユーザ名と POP3 サーバ名より、作成したメールアドレスを使用して、SMTP サーバにメールの送信を要求します。

[未設定時]

メール転送／メール一覧送信の差出人メールアドレスは未設定です。

12.2.8 email send from delete

[機能]

メール転送／メール一覧送信の差出人メールアドレスの削除

[入力形式]

email [<count>] send from delete

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

[説明]

メール転送／メール一覧送信で使用する差出人メールアドレスの設定を削除します。

12.2.9　email send size

[機能]

転送メールサイズの設定

[入力形式]

email [<count>] send size <size>

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0〜9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<size>

- 転送メールサイズ
  転送メールの本文のサイズを、1 バイト〜6144 バイトの 10 進数値で指定します。

[説明]

転送メールの本文のサイズを設定します。

[未設定時]

転送メールサイズとして、6144 バイトを設定したものとみなされます。

```
email <count> send size 6144
```

12.2.10 email send list use

[機能]

メール一覧送信の使用有無の設定

[入力形式]

email [<count>] send list use <mode>

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<mode>

- on
  メール一覧を送信します。
- off
  メール一覧を送信しません。

[説明]

メール一覧を送信するかどうかを設定します。

[未設定時]

メール一覧を送信しないものとみなされます。

```
email <count> send list use off
```

12.2.11　email send list format

[機能]

メール一覧フォーマットの設定

[入力形式]

email [<count>] send list format <format>

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0〜9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<format>

- 0
  1 件を複数行のフォーマットで送信します。
- 1
  1 件を 1 行のフォーマットで送信します。

[説明]

メール一覧のフォーマットを設定します。

[未設定時]

メール一覧を 1 件を複数行のフォーマットで送信するものとみなされます。

```
email <count> send list format 0
```

12.2.12 email send filter use

[機能]

メールフィルタの使用有無の設定

[入力形式]

email [<count>] send filter use <mode>

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<mode>

- on
  メールフィルタを使用します。
- off
  メールフィルタを使用しません。

[説明]

メールフィルタを使用するかどうかを設定します。

[未設定時]

メールフィルタを使用しないものとみなされます。

```
email <count> send filter use off
```

12.2.13　email send filter default

[機能]

メールフィルタのデフォルト動作の設定

[入力形式]

email [<count>] send filter default <action>

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<action>

- pass
  メールフィルタに一致する条件がない場合は、メールを転送します。
- reject
  メールフィルタに一致する条件がない場合は、メールを転送しません。

[説明]

メールフィルタに一致する条件が存在しない場合の動作を設定します。

[未設定時]

メールフィルタに一致する条件がない場合は、メール転送を行うものとみなされます。

```
email <count> send filter default pass
```

12.3 メールフィルタ情報

12.3.1 email filter

[機能]

メールフィルタの設定

[入力形式]

email [<count>] filter <filter_count> action <action> 動作の設定
email [<count>] filter <filter_count> to [<to>] 宛先の設定
email [<count>] filter <filter_count> from [<from>] 差出人の設定
email [<count>] filter <filter_count> subject [<subject>] 題名の設定

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<filter_count>

- メールフィルタ定義番号
  メールフィルタの優先度を表す番号を、0～39 の 10 進数値で指定します。
  指定した値は、順番にソートされてリナンバリングされます。また、同じ値を持つメールフィルタ定義がすでに存在する場合は、既存の定義を変更します。

<action>

条件と一致した場合の動作を設定します。

- pass
  条件と一致する場合に、メールを転送します。
- reject
  条件と一致する場合に、メールを転送しません。

<to>

- 宛先
  対象とするメールの宛先を指定します。
  半角で最大 40 文字まで入力可能 (全角で最大 20 文字まで入力可能)
  省略した場合は、すでに指定されている設定をクリアするものとみなされます。

<from>

- 差出人
  対象とするメールの差出人を指定します。
  半角で最大 40 文字まで入力可能 (全角で最大 20 文字まで入力可能)
  省略した場合は、すでに指定されている設定をクリアするものとみなされます。

<subject>

- 題名
  対象とするメールの題名を指定します。
  半角で最大 40 文字まで入力可能 (全角で最大 20 文字まで入力可能)
  省略した場合は、すでに指定されている設定をクリアするものとみなされます。

[説明]

メールフィルタを設定します。
メールフィルタは、本装置全体で 40 個まで定義できます。

[未設定時]

メールフィルタは未設定です。

12.3.2 email filter move

[機能]

メールフィルタの優先順序の変更

[入力形式]

email [<count>] filter move <filter_count> <new_filter_count>

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0～9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<filter_count>

- 対象メールフィルタ定義番号
  優先順序を変更するメールフィルタ定義の番号を指定します。

<new_filter_count>

- 移動先メールフィルタ定義番号
  <filter_count>に対する新しい順序を、0～40 の 10 進数値で指定します。
  すでにこの番号を持つ定義が存在する場合には、その定義の前に挿入されます。

[説明]

メールフィルタの優先順序を変更します。

12.3.3　email filter delete

[機能]

メールフィルタの削除

[入力形式]

email [<count>] filter delete <filter_count>

[パラメタ]

<count>

- ユーザ定義番号
  ユーザ定義番号を、0〜9 の 10 進数値で指定します。省略した場合は、0 を指定したものとみなされます。

<filter_count>

- 削除するメールフィルタ定義番号
  削除するメールフィルタ定義番号を指定します。
- all
  すべてのメールフィルタを削除する場合に指定します。

[説明]

メールフィルタを削除します。

12.4 TEL メール情報

12.4.1 email tel use

[機能]

TEL メール使用有無の設定

[入力形式]

email tel use <mode>

[パラメタ]

<mode>

- on
  TEL メールを使用します。
- off
  TEL メールを使用しません。

[説明]

TEL メールを使用するかどうかを設定します。

[未設定時]

TEL メールを使用しないものとみなされます。

```
email tel use off
```

12.4.2　email tel delete

[機能]

TEL メール情報の削除

[入力形式]

email tel delete <port>

[パラメタ]

<port>

アナログポート番号を指定します。省略した場合は、0 を指定したものとみなされます。

- 0
  TEL1 ポート
- 1
  TEL2 ポート
- all
  すべての TEL メール情報を削除する場合に指定します。

[説明]

TEL メール情報を削除します。

12.4.3 email tel send

[機能]

TEL メールの宛先と送信サーバの設定

[入力形式]

email tel [<port>] send <to> <from> <smtp_host> [<smtp_port>]

[パラメタ]

<port>

アナログポート番号を指定します。省略した場合は、0 を指定したものとみなされます。

- 0
  TEL1 ポート
- 1
  TEL2 ポート

<to>

- 宛先メールアドレス
  TEL メールの宛先メールアドレスを、0x21,0x23～0x7e の 80 文字以内の ASCII 文字列で指定します。

<from>

- 差出人メールアドレス
  TEL メールの差出人メールアドレスを、0x21,0x23～0x7e の 80 文字以内の ASCII 文字列で指定します。

<smtp_host>

- メールサーバ名
  TEL メール送信時に使用するメールサーバ (SMTP サーバ) のホスト名を、0x21,0x23～0x7e の 80 文字以内の ASCII 文字列で指定します。
  ホスト名を指定した場合は、本装置が DNS サーバを使用可能な状態でなければなりません。
- メールサーバ IP アドレス
  TEL メール送信時に使用するメールサーバ (SMTP サーバ) の IP アドレスを指定します。

<smtp_port>

- ポート番号
  メールサーバ (SMTP サーバ) のポート番号を、1～65535 の 10 進数値で指定します。省略した場合は、25 を指定したものとみなされます。

[説明]

TEL メールの送信サーバに関する情報を設定します。

[未設定時]

TEL メール送信サーバに関する情報は未設定です。

12.4.4　email tel send delete

[機能]

TEL メールの宛先と送信サーバの削除

[入力形式]

email tel [<port>] send delete

[パラメタ]

<port>

アナログポート番号を指定します。省略した場合は、0 を指定したものとみなされます。

- 0
  TEL1 ポート
- 1
  TEL2 ポート

[説明]

TEL メール送信情報を削除します。

12.4.5 email tel auth

[機能]

TEL メールの認証情報の設定

[入力形式]

email tel [<port>] auth use <mode>
email tel [<port>] auth server <host> [<pop3_port>]
email tel [<port>] auth type <type>
email tel [<port>] auth user <user> <pass> [encrypted]

[パラメタ]

<port>

アナログポート番号を指定します。省略した場合は、0 を指定したものとみなされます。

- 0
  TEL1 ポート
- 1
  TEL2 ポート

<mode>

- on
  メール送信の前に POP 認証を行います。
- off
  メール送信の前に POP 認証を行いません。

<host>

- メールサーバ名
  認証するメールサーバ (POP サーバ) のホスト名を、0x21,0x23～0x7e の 80 文字以内の ASCII 文字列で指定します。
  ホスト名を指定した場合は、本装置が DNS サーバを使用可能な状態でなければなりません。
- メールサーバ IP アドレス
  認証するメールサーバ (POP サーバ) のホストの IP アドレスを指定します。

<pop3_port>

- ポート番号
  メールサーバ (POP3 サーバ) のポート番号を、1～65535 の 10 進数値で指定します。
  省略した場合は、110 を指定したものとみなされます。

<type>

- pop
  POP の認証方式で USER / PASS コマンドを使用します。
- apop
  POP の認証方式で APOP コマンドを使用します。

<user>

- ユーザ名
  認証に使用するユーザ名を、0x21,0x23～0x7e の 32 文字以内の ASCII 文字列で指定します。

<pass>

- パスワード
  認証に使用するパスワードを、0x21,0x23～0x7e の 32 文字以内の ASCII 文字列で指定します。
- 暗号化されたパスワード
  show コマンドで表示される暗号化されたパスワードを encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。

encrypted

- 暗号化パスワード指定
  <pass>に暗号化されたパスワードを指定する場合に指定します。

[説明]

TEL メール送信前に行う認証情報に関する設定を行います。
別プロバイダ経由で TEL メールを送信する場合、SPAM などの不正メール対策により、メールの送信が行えない場合があります。
プロバイダによっては、メール送信する前に POP 認証を行えばメール送信が行える (POP before SMTP 方式) 場合があり、この場合には、本コマンドで認証情報を設定することにより、TEL メールの送信ができます。

[注意]

show コマンドでは、暗号化されたパスワードが encrypted と共に表示されます。
show email tel [<port>] auth user を実行すると、暗号化していないパスワードが表示されます。

[未設定時]

TEL メールの送信前に POP 認証を行わないものとみなされます。
POP の認証方式で USER/PASS コマンドを使用するものとみなされます。
ユーザ名およびメールサーバ名は設定しないものとみなされます。

```
email tel <port> auth use off
email tel <port> auth type pop
```

12.4.6 email tel interval

[機能]

TEL メールの送信間隔の設定

[入力形式]

email tel [<port>] interval <time>

[パラメタ]

<port>

アナログポート番号を指定します。省略した場合は、0 を指定したものとみなされます。

- 0
  TEL1 ポート
- 1
  TEL2 ポート

<time>

- 送信間隔
  送信間隔を、18000 秒 (5 分)～604800 秒 (7 日) の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。

[説明]

TEL メールの送信間隔を設定します。
送信間隔を設定しない場合は、着信ごとに TEL メールを送信します。

[未設定時]

TEL メールの送信間隔を設定しない（着信ごとに TEL メールを送信する）ものとみなされます。

12.4.7　email tel interval delete

[機能]

TEL メールの送信間隔の削除

[入力形式]

email tel [<port>] interval delete

[パラメタ]

<port>

アナログポート番号を指定します。省略した場合は、0 を指定したものとみなされます。

- 0
  TEL1 ポート
- 1
  TEL2 ポート

[説明]

TEL メールの送信間隔の設定情報を削除します。
送信間隔を設定しない場合は、着信ごとに TEL メールを送信します。

12.4.8 email tel info

[機能]

TEL メールの送信内容の設定

[入力形式]

email tel [<port>] info <format>

[パラメタ]

<port>

アナログポート番号を指定します。省略した場合は、0 を指定したものとみなされます。

- 0
  TEL1 ポート
- 1
  TEL2 ポート

<format>

- default
  発信者番号、着信番号と着信時刻を送信します。
- out
  発信者番号と着信時刻を送信します。

[説明]

TEL メールの送信内容を設定します。

[未設定時]

発信者番号と着信番号を送信するものとみなされます。

```
email tel <port> info default
```

第 13 章　アナログ情報の設定

13.1　アナログ共通情報

13.1.1　analog isdn number

[機能]

自局電話番号の設定

[入力形式]

analog isdn number <number>

[パラメタ]

<number>

- 自局電話番号
  自局電話番号を、0〜9 の数字と、*、#、-、(、)、\の文字で構成される 32 桁以内の ASCII 文字列で指定します。
- delete
  自局電話番号を削除します。

[説明]

指定した電話番号は、発信者番号通知機能を使用する場合、アナログ発信時に網に通知されます。また、着信時には網から自局番号が通知されない場合、当番号を syslog にて表示します。
INS ボイスワープ／INS ボイスワープセレクト機能使用時には必ず設定してください。

[未設定時]

自局電話番号は未設定です。

13.1.2 analog dial timer

[機能]

ダイヤル桁間タイマの設定

[入力形式]

analog dial timer <value>

[パラメタ]

<value>

ダイヤル桁間タイマとして、以下のいずれかを指定します。

- 5
  ダイヤル桁間タイマとして 5 秒を設定します。
- 8
  ダイヤル桁間タイマとして 8 秒を設定します。
- 10
  ダイヤル桁間タイマとして 10 秒を設定します。
- 15
  ダイヤル桁間タイマとして 15 秒を設定します。
- 20
  ダイヤル桁間タイマとして 20 秒を設定します。

[説明]

アナログ発信時において、ダイヤル後、このタイマ満了時に発信します。

[未設定時]

ダイヤル桁間タイマとして、5 秒を設定したものとみなされます。

```
analog dial timer 5
```

13.1.3　analog hooking timer

[機能]

フッキング認識時間の設定

[入力形式]

analog hooking timer <mode>

[パラメタ]

<mode>

フッキング認識時間として、以下のいずれかを指定します。

- normal
  フックオン検出後、0.3 秒～1.0 秒以内にフックオフを検出する場合、フッキングと認識します。[標準モード]
- fast
  フックオン検出後、0.1 秒～1.0 秒以内にフックオフを検出する場合、フッキングと認識します。[早いモード]
- slow
  フックオン検出後、0.5 秒～1.5 秒以内にフックオフを検出する場合、フッキングと認識します。[遅いモード]

[説明]

フッキング認識時間を設定します。フックオン検出後、フッキング時間の最小値未満でフックオンを検出する場合は、フック状態のノイズとみなして無視します。

[未設定時]

フッキング認識時間として、標準モード を設定したものとみなされます。

```
analog hooking timer normal
```

13.1.4 analog function

[機能]

機能ボタン (#ボタン) 使用有無の設定

[入力形式]

analog function # <mode>

[パラメタ]

<mode>

- mode1
  機能ボタンとして、#ボタン 1 回押下を使用します。
- mode2
  機能ボタンとして、#ボタン 2 回押下を使用します。
- off
  機能ボタンを使用しません。

[説明]

「#」ボタンを機能ボタンとして使用するかどうかを設定します。

[未設定時]

機能ボタンとして、#ボタン 1 回押下を使用するものとみなされます。

```
analog function # mode1
```

13.1.5　analog ir

[機能]

アナログ着信時リング音の設定

[入力形式]

analog ir out <ring> 外線リング音の設定
analog ir in <ring> 内線リング音の設定
analog ir discrimination <ring> 相手電話番号識別リング音の設定
analog ir line <ring> 契約者回線番号識別リング音の設定
analog ir dialin1 <ring> ポート 1 ダイヤルイン番号識別リング音の設定
analog ir dialin2 <ring> ポート 2 ダイヤルイン番号識別リング音の設定
analog ir in1 <ring> 鳴り分け番号 1 識別リング音の設定
analog ir in2 <ring> 鳴り分け番号 2 識別リング音の設定
analog ir in3 <ring> 鳴り分け番号 3 識別リング音の設定

[パラメタ]

<ring>

- ring1
  リング音 1 を使用します。
- ring2
  リング音 2 を使用します。
- ring3
  リング音 3 を使用します。

[説明]

各種リング音 (外線 / 内線 / 相手電話番号識別 / 契約者番号識別 / ダイヤルイン番号識別 / 鳴り分け番号識別) を設定します。

[未設定時]

アナログ着信時リング音として、それぞれ以下を設定したものとみなされます。

```
analog ir out ring1
analog ir in ring2
analog ir discrimination ring3
analog ir line ring1
analog ir dialin1 ring3
analog ir dialin2 ring3
analog ir in1 ring1
analog ir in2 ring3
analog ir in3 ring3
```

13.1.6 analog numlist add

[機能]

アナログ着信識別情報の設定

[入力形式]

analog numlist add <name> <mode> [<number> [<subaddress>]]

[パラメタ]

<name>

- 識別定義名
  登録する識別着信情報の名称を、0x21,0x23～0x7e の 16 文字以内の ASCII 文字列で指定します。
- default
  デフォルト定義を変更する場合に指定します。

<mode>

動作モードとして、以下のいずれかを指定します。

- all
  両ポート呼び出し
- port1
  ポート 1 のみ呼び出し
- port2
  ポート 2 のみ呼び出し
- pri_port1
  ポート 1 優先で呼び出し
- pri_port2
  ポート 2 優先で呼び出し
- refuse
  着信拒否する

<number>

- 相手電話番号
  相手電話番号を、0～9 の数字と、*、#、-、(、)、\の文字で構成される 32 桁以内の ASCII 文字列で指定します。
  識別定義名が"default"の場合には無視されます。

<subaddress>

- 相手サブアドレス
  必要に応じて、着信相手を識別するためのサブアドレスを、半角英数字 19 文字以内で指定します。識別定義名が"default"の場合には無視されます。

[説明]

着信識別情報を設定します。

[未設定時]

アナログ着信識別情報のデフォルト定義として、両ポート呼び出しを設定したものとみなされます。

```
analog numlist add default all
```

13.1.7 analog numlist delete

[機能]

アナログ着信識別情報の削除

[入力形式]

analog numlist delete <name>

[パラメタ]

<name>

削除する着信識別情報の識別定義名を指定します。

- 識別定義名
  削除する着信識別情報の識別定義名を指定します。
- all
  すべての着信識別情報を削除します。

[説明]

着信識別情報を削除します。

13.1.8　analog priority count

[機能]

識別着信時の優先ポートリング回数設定

[入力形式]

analog priority count <value>

[パラメタ]

<value>

- 優先ポートリング回数
  優先ポートとして指定したポートのみ呼び出すリング回数を、1〜10 の 10 進数値で指定します。

[説明]

優先ポートとして指定したポートのみ呼び出すリング回数を設定します。指定回数呼び出しても受話器を取らない場合は、両ポートの呼び出しを行います。
優先ポート着信の設定を行っていない場合は無視されます。

[未設定時]

識別着信時の優先ポートリング回数として、5 回を設定したものとみなされます。

```
analog priority count 5
```

13.1.9 analog flex pseudo

[機能]

疑似フレックスホン機能使用有無の設定

[入力形式]

analog flex pseudo <mode>

[パラメタ]

<mode>

- on
  疑似フレックスホンを使用します。
- off
  疑似フレックスホンを使用しません。

[説明]

疑似フレックスホンを使用するかどうかを設定します。

[未設定時]

疑似フレックスホンを使用しないものとみなされます。

```
analog flex pseudo off
```

13.1.10　analog flex 3party

[機能]

フレックスホン三者通話機能使用有無の設定

[入力形式]

analog flex 3party <mode>

[パラメタ]

<mode>

- on
  フレックスホン三者通話を使用します。
- off
  フレックスホン三者通話を使用しません。

[説明]

フレックスホン三者通話機能を使用するかどうかを設定します。

[未設定時]

フレックスホン三者通話機能を使用しないものとみなされます。

```
analog flex 3party off
```

13.1.11 analog flex call trans

[機能]

フレックスホン通信中転送機能使用有無の設定

[入力形式]

analog flex call trans <mode>

[パラメタ]

<mode>

- on
  フレックスホン通信中転送を使用します。
- off
  フレックスホン通信中転送を使用しません。

[説明]

フレックスホン通信中転送機能を使用するかどうかを設定します。

[未設定時]

フレックスホン通信中転送機能を使用しないものとみなされます。

```
analog flex call trans off
```

13.1.12　analog flex call deflection

[機能]

フレックスホン着信転送機能の設定

[入力形式]

analog flex call deflection use <mode> フレックスホン着信転送機能の使用有無の設定
analog flex call deflection line <number> 契約者番号の転送先の設定
analog flex call deflection port1 <number> ポート 1 のダイヤルインの転送先の設定
analog flex call deflection port2 <number> ポート 2 のダイヤルインの転送先の設定
analog flex call deflection in1 <number> 鳴り分け番号 1 の転送先の設定
analog flex call deflection in2 <number> 鳴り分け番号 2 の転送先の設定
analog flex call deflection in3 <number> 鳴り分け番号 3 の転送先の設定
analog flex call deflection mtalkie <talkie> 転送元トーキの使用有無の設定
analog flex call deflection otalkie <talkie> 転送トーキを使用有無の設定

[パラメタ]

<mode>

- on
  着信転送を使用します。
- off
  着信転送／疑似着信転送を使用しません。
- pseudo
  疑似着信転送を使用します。

<number>

- 転送先番号
  転送先の電話番号を、0～9 の数字と、*、#、-、(、)、\の文字で構成される 32 桁以内の ASCII 文字列で指定します。
- delete
  転送先番号を削除します。

<talkie>

- on
  トーキを使用します。
- off
  トーキを使用しません。

[説明]

フレックスホン着信転送機能の使用有無、転送先番号、およびトーキの使用有無を設定します。
転送先番号が未設定の場合、着信転送機能を使用するに設定していても転送は行われません。

[未設定時]

フレックスホン着信転送機能を使用しないものとみなされます。

```
analog flex call deflection use off
analog flex call deflection mtalkie off
analog flex call deflection otalkie off
```

13.1.13　analog password

[機能]

アナログ設定変更用暗証番号の設定

[入力形式]

analog password <number> [encrypted]

[パラメタ]

<number>

- 暗証番号
  外線からの設定変更時に使用する暗証番号を、0～9 までの数字 4 桁で指定します。
- 暗号化された暗証番号
  show コマンドで表示される暗号化された暗証番号を encrypted と共に指定します。
  show コマンドで表示される文字列をそのまま正確に指定してください。
- delete
  暗証番号を削除します。

encrypted

- 暗号化暗証番号指定
  <number>に暗号化された認証番号を指定する場合に指定します。

[説明]

リモートの ISDN 機器 (電話機など) から設定変更を行う際の暗証番号を設定します。
本装置のアナログポートに接続された電話機から設定変更を行う場合、暗証番号は不要です。
show コマンドでは、暗号化された暗証番号が encrypted と共に表示されます。
show analog password を実行すると、暗号化していない暗証番号が表示されます。
ここで設定した暗証番号を以下のように使用します。
操作例 1) リモートの ISDN 機器から設定を変更する (暗証番号設定あり)。

- 着信転送機能 ON 設定
  (自側ダイヤル番号)*(暗証番号)6001
- 着信転送機能 OFF 設定
  (自側ダイヤル番号)*(暗証番号)6002
- 省電力モード 遷移設定
  (自側ダイヤル番号)*(暗証番号)8001
- 省電力モード 解除設定
  (自側ダイヤル番号)*(暗証番号)8002

操作例 2) 本装置のアナログポートに接続された電話機から設定を変更する (暗証番号設定は無効)。

- 着信転送機能 ON 設定
  *0*6001

[未設定時]

設定変更用暗証番号は未設定です。

13.1.14 analog inumber

[機能]

i・ナンバー機能の設定

[入力形式]

analog inumber use <mode> i・ナンバー機能の使用有無の設定
analog inumber in1 <port> [<number>] i・ナンバー情報 1 の設定
analog inumber in2 <port> [<number>] i・ナンバー情報 2 の設定
analog inumber in3 <port> [<number>] i・ナンバー情報 3 の設定

[パラメタ]

<mode>

- on
  i・ナンバーを使用します。
- off
  i・ナンバーを使用しません。

<port>

動作モードとして、以下のいずれかを指定します。

- all
  両ポート呼び出し
- port1
  ポート 1 のみ呼び出し
- port2
  ポート 2 のみ呼び出し
- refuse
  着信拒否

<number>

- 鳴り分け番号
  鳴り分け番号を、0～9 の数字と、*、#、-、(、)、\の文字で構成される 32 桁以内の ASCII 文字列で指定します。
  鳴り分け番号を消去または省略する場合は、パラメタを省略してください。

[説明]

i・ナンバーを使用するかどうかを設定します。
i・ナンバーを使用する場合、i・ナンバー情報の設定が有効になります。

[未設定時]

i・ナンバー機能を使用しないものとみなされます。

```
analog inumber off
analog inumber in1 port1
analog inumber in2 port2
analog inumber in3 all
```

13.1.15　analog discern use

[機能]

アナログ着信時識別リング音の使用モード の設定

[入力形式]

analog discern use <mode>

[パラメタ]

<mode>

- self
  着信電話番号の識別リング音を使用します。
- other
  相手電話番号の識別リング音を使用します。

[説明]

アナログ着信時識別リング音の使用モード を設定します。

[未設定時]

相手電話番号の識別リング音を使用するものとみなされます。

```
analog discern use other
```

13.1.16 analog convert

[機能]

アナログダイヤルイン、モデムダイヤルイン時の送出番号の設定

[入力形式]

analog convert use <mode> アナログダイヤルイン、モデムダイヤルイン時の番号送出方法の設定
analog convert line <number> 契約者回線番号で着信時の送出番号の設定
analog convert dialin1 <number> ポート 1 ダイヤルイン番号で着信時の送出番号の設定
analog convert dialin2 <number> ポート 2 ダイヤルイン番号で着信時の送出番号の設定
analog convert in1 <number> 鳴り分け番号 1 で着信時の送出番号の設定
analog convert in2 <number> 鳴り分け番号 2 で着信時の送出番号の設定
analog convert in3 <number> 鳴り分け番号 3 で着信時の送出番号の設定

[パラメタ]

<mode>

- on
  <number>で指定する送出番号を送出します。
- off
  網から通知された番号をそのまま送出します。

<number>

- 送出番号
  送出する番号を、0～9 の数字と、*、#、-、(、)、\の文字で構成される 32 桁以内の ASCII 文字列で指定します。
  アナログダイヤルインの場合は、最後の 4 桁だけ有効となります。

[説明]

アナログダイヤルイン、モデムダイヤルイン時に、アナログポートへ送出する着信番号について設定します。網から通知された番号、または<number>に設定した番号を送出します。
analog convert use on と設定した場合に、<number>に指定する送出番号が有効となります。

[未設定時]

アナログダイヤルイン、モデムダイヤルイン時に、網から通知された番号をそのまま送出します。

```
analog convert use off
```

13.1.17　analog homeout use

[機能]

留守状態の設定

[入力形式]

analog homeout use <mode>

[パラメタ]

<mode>

- on
  留守状態を設定します（留守）。
- off
  留守状態を取り消します（在宅）。

[説明]

留守状態の設定を行います。「留守」を設定した場合、外線からサブアドレス (留守確認用番号) 付き発信することで、無課金で留守状態を確認することができます。留守確認用番号の設定が必要です。

[未設定時]

留守状態は未設定（在宅）です。

```
analog homeout use off
```

13.1.18 analog homeout check

[機能]

留守確認用番号の設定

[入力形式]

analog homeout check <number>

[パラメタ]

<number>

- 留守確認用番号
  留守確認に使用する確認番号を、0～9 の数字 4 桁で指定します。
- delete
  留守確認用番号を削除します。

[説明]

留守確認に使用する確認番号を設定します。

[未設定時]

留守確認用番号は未設定です。

13.1.19　analog noid accept

[機能]

発信者番号非通知着信の設定

[入力形式]

analog noid accept <mode>

[パラメタ]

<mode>

動作モードとして、以下のいずれかを指定します。

- all
  両ポート呼び出し
- port1
  ポート 1 のみ呼び出し
- port2
  ポート 2 のみ呼び出し
- pri_port1
  ポート 1 優先で呼び出し
- pri_port2
  ポート 2 優先で呼び出し
- refuse
  着信拒否

[説明]

発信番号非通知着信の動作モードを設定します。

[未設定時]

発信番号非通知着信の動作モードとして、両ポート呼び出しを設定したものとみなされます。

```
analog noid accept all
```

13.1.20 analog pubtel accept

[機能]

公衆電話着信の設定

[入力形式]

analog pubtel accept <mode>

[パラメタ]

<mode>

動作モードとして、以下のいずれかを指定します。

- all
  両ポート呼び出し
- port1
  ポート 1 のみ呼び出し
- port2
  ポート 2 のみ呼び出し
- pri_port1
  ポート 1 優先で呼び出し
- pri_port2
  ポート 2 優先で呼び出し
- refuse
  着信拒否

[説明]

公衆電話着信の動作モードを設定します。

[未設定時]

公衆電話着信の動作モードとして、両ポート呼び出しを設定したものとみなされます。

```
analog pubtel accept all
```

13.2　アナログポート情報

13.2.1　tel kind

[機能]

ポート接続機器種別の設定

[入力形式]

tel <port> kind <kind>

[パラメタ]

<port>

- アナログポート番号
  1 または 2 を指定します。

<kind>

- no
  接続機器なし
- tel
  電話接続
- modem
  モデム接続
- fax
  FAX 接続
- dsfax
  識別無鳴動 FAX 接続:着信時高位レイヤ情報によって 1300Hz 信号送出
- fsfax
  強制無鳴動 FAX 接続:着信時 1300Hz 信号送出
- catchfax
  キャッチホン可能な FAX：発信時 FAX の動作となり、着信時電話の動作となります。

[説明]

指定したアナログポートに接続するアナログ機器の種別を設定します。

[未設定時]

ポート接続機器種別として、電話接続を設定したものとみなされます。

```
tel 1 kind tel
tel 2 kind tel
```

13.2.2 tel global

[機能]

グローバル着信の設定

[入力形式]

tel <port> global <mode>

[パラメタ]

<port>

- アナログポート番号
  1 または 2 を指定します。

<mode>

- on
  グローバル着信を行います。
- off
  グローバル着信を行いません。

[説明]

指定したアナログポートにてグローバル着信するかどうかを設定します。

[未設定時]

グローバル着信を行うものとみなされます。

```
tel 1 global on
tel 2 global on
```

13.2.3　tel dialin

[機能]

ダイヤルイン番号の設定

[入力形式]

tel <port> dialin <number>

[パラメタ]

<port>

- アナログポート番号
  1 または 2 を指定します。

<number>

- ダイヤルイン番号
  ダイヤルイン番号を、0〜9 の数字と、*、#、-、(、)、\の文字で構成される 32 桁以内の ASCII 文字列で指定します。
- delete
  ダイヤルイン番号を削除します。

[説明]

指定したアナログポートのダイヤルイン番号を設定します。

[未設定時]

ダイヤルイン番号は未設定です。

13.2.4 tel subaddress

[機能]

サブアドレスの設定

[入力形式]

tel <port> subaddress <subaddress>

[パラメタ]

<port>

- アナログポート番号
  1 または 2 を指定します。

<subaddress>

- サブアドレス
  サブアドレスを、半角英数字 19 文字以内で指定します。
- delete
  サブアドレスを削除します。

[説明]

指定したアナログポートのサブアドレスを設定します。

[未設定時]

サブアドレスは未設定です。

13.2.5　tel numbersend

[機能]

発信者番号通知機能の使用有無の設定

[入力形式]

tel <port> numbersend <mode>

[パラメタ]

<port>

- アナログポート番号
  1 または 2 を指定します。

<mode>

- on
  発信者番号の通知を行います。
- off
  発信者番号の通知を行いません。
- net
  網契約に従います。

[説明]

指定したアナログポートにて発信者番号通知機能を使用するかどうかを設定します。

[未設定時]

発信者番号通知は、網契約に従うものとみなされます。

```
tel 1 numbersend net
tel 2 numbersend net
```

13.2.6 tel callmode

[機能]

発着信専用の設定

[入力形式]

tel <port> callmode <callmode>

[パラメタ]

<port>

- アナログポート番号
  1 または 2 を指定します。

<callmode>

- in
  着信専用とする場合に指定します。
- out
  発信専用とする場合に指定します。
- inout
  発着信可能とする場合に指定します。

[説明]

指定したアナログポートの発着信動作を設定します。

[未設定時]

アナログポートの発着信動作として、発着信可能を設定したものとみなされます。

```
tel 1 callmode inout
tel 2 callmode inout
```

13.2.7　tel numberdisplay

[機能]

通信前情報通知機能使用有無の設定

[入力形式]

tel <port> numberdisplay <mode>

[パラメタ]

<port>

- アナログポート番号
  1 または 2 を指定します。

<mode>

- off
  ナンバーディスプレイ機能を使用しません。
- mode1
  ナンバーディスプレイモード 1
- mode2
  ナンバーディスプレイモード 2
- modem1
  モデムダイヤルインモード 1
- modem2
  モデムダイヤルインモード 2
- analog
  アナログダイヤルインモード
- ndmodem1
  モード 1 のナンバーディスプレイとモデムダイヤルイン
- ndmodem2
  モード 2 のナンバーディスプレイとモデムダイヤルイン

[説明]

指定したアナログポートにおける情報通知方式を設定します。

[未設定時]

ナンバーディスプレイ機能を使用しないものとみなされます。

```
tel 1 numberdisplay off
tel 2 numberdisplay off
```

13.2.8 tel call waiting

[機能]

キャッチホン機能の設定

[入力形式]

tel <port> call waiting <mode>

[パラメタ]

<port>

- アナログポート番号
  1 または 2 を指定します。

<mode>

- on
  キャッチホン機能を使用します。
- off
  キャッチホン機能を使用しません。
- pseudo
  疑似キャッチホン機能を使用します。

[説明]

指定したアナログポートにてキャッチホンを使用するかどうかを設定します。

[未設定時]

キャッチホン機能を使用しないものとみなされます。

```
tel 1 call waiting off
tel 2 call waiting off
```

13.2.9　tel volume

[機能]

受話音量の設定

[入力形式]

tel <port> volume <mode>

[パラメタ]

<port>

- アナログポート番号
  1 または 2 を指定します。

<mode>

受話音量として、以下のいずれかを指定します。

- max
  大音量
- mid
  中音量
- min
  小音量

[説明]

指定したアナログポートの受話音量を設定します。

[未設定時]

アナログポートの受話音量として、中音量を設定したものとみなされます。

```
tel 1 volume mid
tel 2 volume mid
```

13.2.10 tel rpuls

[機能]

リバースパルス機能の設定

[入力形式]

tel <port> rpuls <mode>

[パラメタ]

<port>

- アナログポート番号
  1 または 2 を指定します。

<mode>

- on
  リバースパルス機能を使用します。
- off
  リバースパルス機能を使用しません。

[説明]

指定したアナログポートにてリバースパルス信号を送出するかどうかを設定します。

[未設定時]

リバースパルス機能を使用しないものとみなされます。

```
tel 1 rplus off
tel 2 rplus off
```

13.2.11　tel denylist add

[機能]

外線発信を抑止する局番または電話番号の設定

[入力形式]

tel <port> denylist add <number>

[パラメタ]

<port>

- アナログポート番号
  1 または 2 を指定します。

<number>

- 発信抑止電話番号
  発信抑止電話番号を、0〜9 の数字と、*、#、-、(、)、\の文字で構成される 32 桁以内の ASCII 文字列で指定します。

[説明]

指定したアナログポートにおける発信抑止電話番号を設定します。

[未設定時]

発信抑止電話番号は未設定です。

13.2.12 tel denylist delete

[機能]

外線発信を抑止する局番または電話番号の削除

[入力形式]

tel <port> denylist delete <number>

[パラメタ]

<port>

- アナログポート番号
  1 または 2 を指定します。

<number>

削除する発信抑止電話番号を指定します。

- 発信抑止電話番号
  削除する発信抑止電話番号を指定します。
- all
  すべての発信抑止電話番号を削除する場合に指定します。

[説明]

指定したアナログポートにおける発信抑止電話番号を削除します。

13.2.13　tel permitlist add

[機能]

外線発信を許可する局番または電話番号の設定

[入力形式]

tel <port> permitlist add <number>

[パラメタ]

<port>

- アナログポート番号
  1 または 2 を指定します。

<number>

- 発信許可電話番号
  発信許可電話番号を、0〜9 の数字と、*、#、-、(、)、\の文字で構成される 32 桁以内の ASCII 文字列で指定します。

[説明]

指定したアナログポートにおける発信許可電話番号を設定します。

[未設定時]

発信許可電話番号は未設定です。

13.2.14 tel permitlist delete

[機能]

外線発信を許可する局番または電話番号の削除

[入力形式]

tel <port> permitlist delete <number>

[パラメタ]

<port>

- アナログポート番号
  1 または 2 を指定します。

<number>

削除する発信許可電話番号を指定します。

- 発信許可電話番号
  削除する発信許可電話番号を指定します。
- all
  すべての発信許可電話番号を削除する場合に指定します。

[説明]

指定したアナログポートにおける発信許可電話番号を削除します。

13.2.15　tel autoswitch

[機能]

フレックスホン自動切り替え機能使用有無の設定

[入力形式]

tel <port> autoswitch <mode>

[パラメタ]

<port>

- アナログポート番号
  1 または 2 を指定します。

<mode>

- on
  自動切り替え機能を使用します。
- off
  自動切り替え機能を使用しません。

[説明]

指定したアナログポートにてフレックスホン自動切り替え機能を使用するかどうかを設定します。

[未設定時]

フレックスホン自動切り替え機能を使用しないものとみなされます。

```
tel 1 autoswitch off
tel 2 autoswitch off
```

13.2.16 tel catchdisplay

[機能]

キャッチホン・ディスプレイ機能使用有無の設定

[入力形式]

tel <port> catchdisplay <mode>

[パラメタ]

<port>

- アナログポート番号
  1 または 2 を指定します。

<mode>

- off
  キャッチホン・ディスプレイ機能を使用しません。
- mode1
  キャッチホン・ディスプレイ (モード 1) を使用します。
- mode2
  キャッチホン・ディスプレイ (モード 2) を使用します。
- mode3
  キャッチホン・ディスプレイ (モード 3) を使用します。
- mode4
  キャッチホン・ディスプレイ (モード 4) を使用します。

[説明]

指定したアナログポートにてキャッチホンのナンバー・ディスプレイを使用するかどうかを設定します。

[未設定時]

キャッチホン・ディスプレイ機能を使用しないものとみなされます。

```
tel 1 catchdisplay off
tel 2 catchdisplay off
```

13.2.17　tel catchtone

[機能]

通話中着信音送出時間の設定

[入力形式]

tel <port> catchtone <value>

[パラメタ]

<port>

- アナログポート番号
  1 または 2 を指定します。

<value>

通話中着信音送出時間として、以下のいずれかを指定します。

- 0
  無限に送出処理を行います。
- 5
  送出時間として 5 秒を指定します。
- 10
  送出時間として 10 秒を指定します。
- 15
  送出時間として 15 秒を指定します。
- 20
  送出時間として 20 秒を指定します。
- 25
  送出時間として 25 秒を指定します。
- 30
  送出時間として 30 秒を指定します。

[説明]

通話中着信音送出時間を設定します。

[未設定時]

通話中着信音を無限に送出するものとみなされます。

```
tel 1 catchtone 0
tel 2 catchtone 0
```

第 14 章　制御コマンド

14.1　装置の制御

14.1.1　logon

[機能]

コマンド の使用開始の宣言

[入力形式]

logon

[オプション]

なし

[パラメタ]

なし

[説明]

コマンド の使用開始を宣言します。
本コマンド は、シリアルポート に接続されたコンソールから実行できます。

[注意]

シリアルポート に接続されたコンソールから logon している最中に、ほかのプログラムからコマンド を実行することはできません。ほかのプログラムからコマンド を実行する場合は、“14.1.2 exit” を実行して、コンソールでのコマンド 使用を終了してください。

[例]

以下に、実行例を示します。

```
> logon
#
```

14.1.2　exit

[機能]

コマンドの使用終了

[入力形式]

exit

[オプション]

なし

[パラメタ]

なし

[説明]

コンソールからのコマンド操作を終了します。
telnet でリモート端末から使用している場合は、telnet コネクションを切断します。

[例]

以下に、実行例を示します。

```
# exit
>
```

14.1.3 save

[機能]

構成定義情報の保存

[入力形式]

save

[オプション]

なし

[パラメタ]

なし

[説明]

構成定義情報を保存します。
構成定義コマンドによって設定または変更した構成定義情報を、FLASH メモリに格納します。
格納する構成定義情報のサイズが、FLASH メモリ上の構成定義保存領域のサイズを超えていた場合は、以下のエラーメッセージを出力します。また、FLASH メモリへの格納は行われません。

```
save failed: config too big
```

[例]

以下に、実行例を示します。

```
# save
```

14.1.4　enable

[機能]

構成定義情報の動的変更

[入力形式]

enable

[オプション]

なし

[パラメタ]

なし

[説明]

各コマンドで設定または変更した構成定義情報を、装置の再起動を行わずに有効にします。
wan line を設定した場合、以下のエラーメッセージを表示し、動的定義変更はできません。
reset で再起動してください。

```
enable: need reset
```

[注意]

enable コマンドを実行した場合、装置内部のアドレス情報などを再設定するために、いったん、通信インタフェースをダウンさせます。そのため、enable コマンド実行時に通信が途切れますので注意してください。
なお、アナログ通話は切断されません。
また、enable コマンド実行時に以下の IP アドレス重複のメッセージが出た場合は、IP アドレスを修正後、reset コマンドを実行してください。
lan <no> has same network / address as lan <other_no> (<no>,<other_no>は lan 定義番号)
remote <no> has same remote address as remote <other_no> (<no>,<other_no>は相手定義番号)

[例]

以下に、実行例を示します。

```
# enable
```

14.1.5 reset

[機能]

装置の再起動

[入力形式]

reset [<mode>]

[オプション]

なし

[パラメタ]

<mode>

再起動のモードを指定します。

- clear
  設定をご購入時の状態に戻し、装置を再起動します。
- config1
  構成定義 1 に切り替えて、装置を再起動します。
- config2
  構成定義 2 に切り替えて、装置を再起動します。

[説明]

装置を再起動します。
構成定義情報を変更した場合は、本コマンドを実行して装置を再起動してください。変更した内容は、再起動後に有効となります。
装置を再起動せずに変更した内容を有効にしたい場合は、“14.1.4 enable” を実行します。

[例]

以下に、実行例を示します。

```
# reset
```

14.1.6　update

[機能]

ファームウェアの更新

[入力形式]

update

[オプション]

なし

[パラメタ]

なし

[説明]

ファームウェア更新情報に従って他システムからファームウェアを読み込み、FLASH メモリの内容を書き替えます。
以下に、ファームウェア更新手順の概要を示します。

1) ファームウェア更新情報を登録します。(""“11.9.1 updateinfo”"参照)

   # updateinfo ....

   # save

2) ファームウェアを更新します。

   # update

3) 装置を再起動します。

   # reset

[例]

以下に、実行例を示します。

```
> logon
# updateinfo 192.168.1.2 sir sir-passwd /SIR/SIRSOFT.ftp
# save
# enable
# update
    --ファイル転送(FTP)--
    --ファイルチェック(md5)--
    --バージョンチェック(エディション番号が同一)--
    --フラッシュROMへの書き込み--
# reset
    --更新したファームウェアでシステムを再起動--
>
```

14.1.7 date

[機能]

絶対時間の設定/表示

[入力形式]

date [<yymmddHHMMSS>]

[オプション]

なし

[パラメタ]

<yymmddHHMMSS>

日付および時刻を指定します。

yyyy 西暦の下 2 桁を指定します。00～36 を指定した場合は、西暦 2000 年以降とみなされます。

mm 月を、1～12 の 10 進数値で指定します。

dd 日付を、1～31 の 10 進数値で指定します。

HH 時間を、0～23 の 10 進数値で指定します。

MM 分を、0～59 の 10 進数値で指定します。

SS 秒を、0～59 の 10 進数値で指定します。

指定した日付と時間は、ローカルタイムで処理されます。

[説明]

絶対時間を設定します。
パラメタなしで本コマンドを実行した場合は、現在の日付と時刻を表示します。
本コマンドをパラメタなしで実行すると、"Fri Jun 27 18:36:53 2008"の形式で現在の日付と時刻が表示されます。
コマンド実行時にパラメタで日付と時刻を指定した場合、その情報を絶対時間として設定します。

[注意]

構成定義情報にタイムゾーン (time zone <offset>) が指定されていない状態では GMT (グリニッジ標準時間) として表示/設定されます。

[例]

以下に、実行例を示します。

- 現在の日付と時刻を設定する場合

```
# date 080716155300
#
```

- 現在の日付と時刻を表示する場合

```
# date
Mon Jun 30 15:53:01 2008
#
```

14.1.8　rdate

[機能]

リモートホストの時刻を本装置の絶対時間に設定

[入力形式]

rdate

[オプション]

なし

[パラメタ]

なし

[説明]

タイムサーバから現在時刻を取得し、本装置の絶対時間として設定します。
“11.3.1 time auto server” で指定したサーバから、現在時刻を取得します。

[例]

以下に、サーバから現在時刻を取得する場合の実行例を示します。

```
# rdate
Mon Jun 30 10:30:00 2008
#
```

14.1.9 dnconv

[機能]

電話番号変更処理の実施

[入力形式]

dnconv <index>

[オプション]

なし

[パラメタ]

<index>

一括変更処理の対象とする、電話番号変更予約情報を指定します。

- 0～3
  電話番号変更予約情報 (dnconvinfo) の登録番号を指定します。
- all
  登録されている電話番号変更情報 (dnconvinfo) すべてを対象とする場合に指定します。

[説明]

電話番号変更予約情報に従って、構成定義情報に登録されている電話番号を一括変更します。

[注意]

本コマンドでは、電話番号一括変更処理後の構成定義情報の保存 (save)、およびシステムのリセット (reset) は行いません。

[例]

以下に、実行例を示します。

- 特定の電話番号変更予約情報の一括変更処理

```
# dnconv 1
 ....
# dnconv 3
 ....
# save
# reset
>
```

- すべての電話番号変更予約情報の一括変更処理

```
# dnconv all
 ....
# save
# reset
>
```

14.1.10　vrrpctl

[機能]

VRRP 機能の制御

[入力形式]

vrrpctl preempt on {<lan_number>|all} [{<vrid>|all} [<interval>]]

[オプション]

なし

[パラメタ]

<lan_number>

コマンド適用対象の LAN インタフェースを指定します。

- lan 定義番号
  lan 定義番号として、0 を指定してください。
- all
  すべての LAN インタフェースを適用対象とする場合に指定します。

<vrid>

コマンド適用対象の VRRP グループを指定します。

- VRID
  対象の LAN インタフェースに設定されている VRRP グループの VRID を、1～255 の 10 進数値で指定します。
- all
  対象の LAN インタフェースに設定されているすべての VRRP グループを適用対象とする場合に指定します。

<interval>

- プリエンプトモード ON 時間
  プリエンプトモードを ON にする時間を、1～900 の範囲で指定します。単位は秒です。省略した場合は、VRRP グループに設定された VRRP-AD 送信間隔の 3 倍+5 秒の時間を指定したものとみなされます。また、VRRP-AD 送信間隔の 3 倍+5 より小さい値を指定しても VRRP-AD 送信間隔の 3 倍+5 秒を指定されたものとして動作します。

[説明]

VRRP グループの動作を、一時的にプリエンプトモードが ON に設定されたものとして動作させます。
これにより、プリエンプトモードが OFF に設定された自装置 VRRP グループが現在のマスタルータより優先度の高いバックアップルータである場合、マスタルータに状態を切り戻すことができます。
コマンドが正常に実行された場合は以下のメッセージを出力します。

```
vrrpctl: command accepted vrid<vrid>
```

<vrid>　コマンドが適用された VRRP グループを示します。

指定された自装置 VRRP グループのプリエンプトモードが ON であったり、現在のマスタルータの優先度のほうが高い場合、要求は無視され以下のエラーメッセージを出力します。なお、VRID が指定されなかった場合はエラーメッセージは出力されません。

```
vrrpctl: not command accept vrid<vrid>
```

<vrid>　コマンドが適用されなかった VRRP グループを示します。

また、有効ではない VRRP グループが指定された場合は以下のエラーメッセージを出力します。

```
vrrpctl: Bad vrid<vrid> provided
```

<vrid>　有効ではない VRRP グループを示します。

[例]

以下に、現在はマスタルータとして動作している待機設定ルータで lan0 の VRID が 10 の VRRP グループを、優先度の高い仮想ルータへきり戻しを行う場合の実行例を示します。

```
# vrrpctl preempt on 0 10
vrrpctl: command accepted vrid10
#
```

14.2　リモート パワーオンの制御

14.2.1　rpon

[機能]

リモート パワーオン機能のための MagicPacket の送信

[入力形式]

rpon <host_number>

[オプション]

なし

[パラメタ]

<host_number>

- ホストデータベース定義番号
  MagicPacket 送出先のホストデータベース定義番号を指定します。
- all
  ホストデータベースに登録されたリモート パワーオン対象の全ホスト。

[説明]

ホストデータベース定義番号により指定されたホストに対して、MagicPacket を送出します。
<host_number>が指定されないか、有効範囲から外れているか、またはそのホスト情報に MAC アドレスが設定されていない場合にはなにもしません。<hosts_number>に all が指定されている場合は、MAC アドレスが設定されておりリモート パワーオン非対象ホストではない全ホストに対して MagicPacket を送出します。

[例]

以下に、実行例を示します。

```
# rpon 2
#
```

14.3 オンラインサポートの制御

14.3.1 rcmdctl

[機能]

オンラインサポートの開始/終了

[入力形式]

rcmdctl start <dial_number> [<subaddress>] オンラインサポートの開始
rcmdctl stop オンラインサポートの終了
rcmdctl status オンラインサポートに関する状態表示

[オプション]

なし

[パラメタ]

<dial_number>

- 相手電話番号
  相手の電話番号を、0〜9 の数字と、*、#、-、(、)、\の文字で構成される 32 桁以内の ASCII 文字列で指定します。

<subaddress>

- 相手サブアドレス
  相手のサブアドレスを、0x21,0x23〜0x7e の文字で構成される 19 桁以内の ASCII 文字列で指定します。

[説明]

センタ側 (保守用) の本装置からリモート側 (遠隔地) に接続された本装置の操作を行う場合に、センタ側でこのコマンドを使用してオンラインサポートの開始/終了を行います。
"rcmdctl start"を指定すると、<dial_number>に指定した電話番号で回線を接続し、接続後はリモート側のコマンド実行が行える状態となります。
"rcmdctl stop"を指定すると、接続中の回線を切断します。
"rcmdctl status"を指定すると、現在の状態を表示します。
リモート側が出荷状態のままの場合 (rcmdinfo が未設定時) は、相手サブアドレス<subaddress> に相手の MAC アドレスを 12 桁で指定します。

[例]

以下に、実行例を示します。

- オンラインサポートを開始する場合

```
# rcmdctl start 0344445555 00000e001234
#
```

- オンラインサポートを終了する場合

```
# rcmdctl stop
#
```

14.3.2　rcmd

[機能]

オンラインサポートによるリモート側の本装置のコマンド実行

[入力形式]

rcmd <command>

[オプション]

なし

[パラメタ]

<command>

- コマンド
  リモート側で実行するコマンド文字列を指定します。

[説明]

センタ側 (保守用) の本装置からリモート側 (遠隔地) に接続された本装置に、コマンドを送信し、リモート側は受信したコマンドを実行します。
コマンドの実施に先だって、rcmdctl コマンドによりオンラインサポートを開始しておかなければなりません。

[例]

以下に、実行例を示します。

- リモート側の本装置のバージョン情報の表示

```
# rcmdctl start 0344445555 00000e001234
# rcmd idinfo
Si-R130B
00000e000001
ROM:1.1
FIRM:V04.07
# rcmdctl stop
```

14.4 E メールエージェントの制御

14.4.1 emailcheck

[機能]

E メールエージェントの制御

[入力形式]

emailcheck [-i <count>]
emailcheck -c [-i <count>]
emailcheck -d -i <count>
emailcheck -r [-i <count>]
emailcheck -r -s <host>[:<port>] -u <user> -p <pass> [-t] [-A]

[オプション]

-r

メールチェックを実行します。

-c

メールチェックで取得したメールの取得件数だけ表示します。
メールの送信者 (From) / 題名 (Subject) / 送信時刻 (Date) は表示されません。

-d

メールチェックで取得したメールの情報を削除します。

-i

ユーザ定義番号を指定します。

-s

接続先のホスト名または IP アドレスを指定します。

-u

メールサーバにアクセスするためのメールアカウントを指定します。

-p

メールサーバにアクセスするためのパスワードを指定します。

-t

メール情報を取得する際にトレース情報を出力します。

-A

サーバとの認証に APOP を使用します。

[パラメタ]

<count>

- ユーザ定義番号 (0〜9)
  email コマンドで設定したユーザ定義番号を、0〜9 の 10 進数値で指定します。
- all
  すべてのユーザ定義番号を対象とします。

<host>

- メールサーバ名

  メールサーバ (POP サーバ) のホスト名を、0x21,0x23～0x7e の 80 文字以内の ASCII 文字列で指定します。

  ホスト名を指定した場合は、本装置が DNS サーバを使用可能な状態でなければなりません。

- メールサーバ IP アドレス

  メールサーバ (POP サーバ) のホストの IP アドレスを指定します。

<port>

- ポート番号

  メールサーバ (POP3 サーバ) のポート番号を、1～65535 の 10 進数値で指定します。

  省略した場合は、110 を指定したものとみなされます。

<user>

- ユーザ名

  メールサーバにアクセスするためのアカウントを、0x21,0x23～0x7e の 32 文字以内の ASCII 文字列で指定します。

<pass>

- パスワード

  メールサーバにアクセスするためのパスワードを、0x21,0x23～0x7e の 32 文字以内の ASCII 文字列で指定します。

[説明]

オプションを指定しない場合、または-i オプションだけを指定した場合、メールチェックで取得したメール情報を表示します。
-r と-s,-u,-p オプションを指定した場合、指定のパラメタに従いメールチェックを実施します。この場合、取得したメール情報は保存されません。
-r オプションのみを指定した場合、email コマンドで設定されているメールチェック情報に従いメールチェックを実施します。
-d オプションを指定した場合、メールチェックで取得したメール情報を削除します。
装置が保持している全メール情報数が 0 になった場合は、CHECK ランプの緑色点滅を消灯します。

[注意]

E メールエージェントが動作中の場合は、メールチェック要求は受け付けられません。

14.5 回線の制御

14.5.1 connect

[機能]

回線接続の指示

[入力形式]

connect <remote_number> <ap_number> [<id> <password>]
connect <ap_name>

[オプション]

なし

[パラメタ]

<remote_number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。

<ap_name>

- アクセスポイント名
  接続するアクセスポイントを指定します。

<id>

- 送信認証 ID(最大 64 文字)

<password>

- 送信認証パスワード (最大 64 文字)

[説明]

指定した接続先 (アクセスポイント) に ISDN を利用して通信する場合に接続処理を行います。
<ap_name>を指定する場合には、同じアクセスポイント名が複数定義されていると一番小さい定義番号のアクセスポイントに対してのみ動作します。
接続ごとに認証 ID、認証パスワードを変更する場合には、<id>、<password>を指定します。

[例]

以下に、tokyo という名前のアクセスポイントと接続する場合の実行例を示します。

```
# connect tokyo
#
```

14.5.2　addlink

[機能]

MP 使用時のチャネル数増加

[入力形式]

addlink <remote_number> <ap_number>
addlink <ap_name>

[オプション]

なし

[パラメタ]

<remote_number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。

<ap_name>

- アクセスポイント名
  アクセスポイントの名前を指定します。

[説明]

MP で 1B 使用時に、チャネル数増加を設定します。

[例]

以下に、実行例を示します。

```
# addlink 0 0
#
```

14.5.3 disconnect

[機能]

回線切断の指示

[入力形式]

disconnect <remote_number> <ap_number>
disconnect <ap_name>

[オプション]

なし

[パラメタ]

<remote_number>

切断する相手定義の番号を指定します。

- 相手定義番号
  相手ネットワークの通し番号を、0～47 の 10 進数値で指定します。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0～47 の 10 進数値で指定します。

<ap_name>

切断するアクセスポイントを指定します。

- アクセスポイント名
  アクセスポイントの名前を指定します。
- all
  すべてのアクセスポイントの切断を行います。

[説明]

指定した接続先 (アクセスポイント) に ISDN を利用して通信する場合に切断処理を行います。
all を指定した場合には、すべての接続先 (アクセスポイント) の切断を行います。

[例]

以下に、tokyo という名前のアクセスポイントと切断する場合の実行例を示します。

```
# disconnect tokyo
#
```

14.5.4　dellink

[機能]

MP 使用時のチャネル数削減

[入力形式]

dellink <remote_number> <ap_number>
dellink <ap_name>

[オプション]

なし

[パラメタ]

<remote_number>

- 相手定義番号
  相手ネットワークの通し番号を、0〜47 の 10 進数値で指定します。

<ap_number>

- アクセスポイント定義番号
  相手ネットワーク内のアクセスポイントの通し番号を、0〜47 の 10 進数値で指定します。

<ap_name>

- アクセスポイント名
  アクセスポイントの名前を指定します。

[説明]

MP で 2B 使用時に、チャネル数を削減します。

[例]

以下に、実行例を示します。

```
# dellink 0 0
#
```

14.5.5 timerctl start

[機能]

回線接続保持タイマの起動

[入力形式]

timerctl start [<time>]

[オプション]

なし

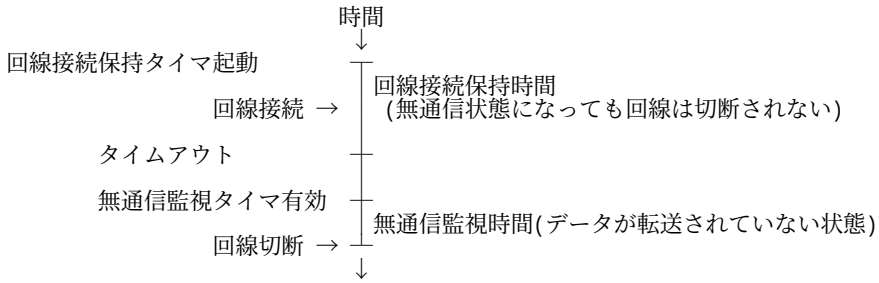
[パラメタ]

<time>

- 回線接続保持時間
  回線接続保持時間を、0 秒～86400 秒 (1 日) の範囲で指定します。
  単位は、d(日)、h(時)、m(分)、s(秒) のいずれかを指定します。

[説明]

回線接続保持タイマを起動します。
本コマンドは、回線が接続されているかどうかに限らず実行できます。
回線接続保持タイマは、本コマンドの実行によって起動し、タイムアウトまたは timerctl stop コマンド (“14.5.6 timerctl stop” を参照) の実行によって停止します。
time を省略した場合には、装置起動 / 再起動 / 設定反映の時点から最初の実行時については wan isdn keep time で設定した値を利用します。それ以外の実行時には前回利用した値が設定されたものとみなされます。
停止後は、無通信監視タイマによる接続時間の監視を再開します。
本コマンドは、回線が接続されているかどうかに限らず実行できます。以下に、回線の未接続時に本コマンドを実行した場合の流れを示します。



[注意]

回線接続保持タイマを起動すると、指定した接続保持時間内は無通信監視タイマによる切断を行いません。ただし、以下の場合には、回線接続を保持することができません。

- “14.5.3 disconnect” で、手動切断した場合
- 相手側から切断された場合
- “5.2.32 remote ap keep” で、「回線接続を保持しない」が設定されている場合 (例: remote 0 ap 0 keep off)

[例]

以下に、回線接続保持時間を 8 時間とする場合の実行例を示します。

```
# timerctl start 8h
#
```

14.5.6 timerctl stop

[機能]

回線接続保持タイマの停止

[入力形式]

timerctl stop

[オプション]

なし

[パラメタ]

なし

[説明]

回線接続保持タイマを停止します。
回線接続保持タイマは、“14.5.5 timerctl start” の実行によって起動され、タイムアウトまたは本コマンドの実行によって停止します。
停止後は、無通信監視タイマによる接続時間の監視を再開します。

[例]

以下に実行例を示します。

```
# timerctl stop
#
```

14.5.7　timerctl remain

[機能]

回線接続保持タイマの残り時間の表示

[入力形式]

timerctl remain

[オプション]

なし

[パラメタ]

なし

[説明]

回線接続保持タイマの残り時間を表示します。
回線接続保持タイマ起動中に本コマンドを実行すると、接続保持時間の残り時間が表示されます。回線接続保持タイマの停止中に本コマンドを実行した場合は、0 が表示されます。

[例]

以下に、回線接続保持タイマの起動中に本コマンドを実行した場合の実行例を示します。

```
# timerctl start 8h
# timerctl remain
7h
#
```

14.6 その他の制御

14.6.1 ping

[機能]

ICMP エコー要求パケットの送信

[入力形式]

ping <host>

[オプション]

なし

[パラメタ]

<host>

エコーテストの対象とする IP アドレスまたはホスト名を指定します。
ホスト名を指定する場合は、ホストデータベース情報に該当するホスト名が登録されているか、または本装置が DNS サーバを使用できる状態でなければなりません。

[説明]

指定したホスト (IP アドレスまたはホスト名) に対して、ICMP ECHO_REQUEST を送信し、ICMP ECHO_RESPONSE の受信を確認します。

[例]

以下に、実行例を示します。

```
# ping 192.168.1.1
ping [192.168.1.1]: 56 data bytes
56 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=3.456
56 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=3.356
56 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=3.455
56 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=3.389
56 bytes from 192.168.1.1: icmp_seq=5 ttl=255 time=3.556
#
```

14.6.2　ping6

[機能]

ICMPv6 エコー要求パケットの送信

[入力形式]

ping6 <address>[%<interface>]

[オプション]

なし

[パラメタ]

<address>

- 送信先 IPv6 address

  ICMPv6 送信先の IPv6 address を指定します。

<interface>

- 送信先インタフェース名

  送信先 IPv6 address が link-local scope の場合に、出力先インタフェースを指定します。link-local scope 以外の IPv6 address 指定時に指定した場合はエラーとなります。

[説明]

指定したホストに対して ICMPv6 ECHO_REQUEST を送信し、ICMPv6 ECHO_RESPONSE の受信を確認します。ホスト名での指定はできません。

[注意]

- ping6 の動作を途中で中断することはできません。
- ping6 の動作中に、CTRL-C を入力しないでください。

[例]

以下に実行例を示します。

```
# ping6 fe80::200:eff:fef1:dc%lan0
ping6 (56=40+8+8 bytes) fe80::200:eff:fef1:efa%lan0 --> fe80::200:eff:fef1:dc%lan0
16 bytes from fe80::200:eff:fef1:efa%lan0 icmp_seq=0 hlim=64 time=0.768ms
16 bytes from fe80::200:eff:fef1:efa%lan0 icmp_seq=0 hlim=64 time=0.691ms
16 bytes from fe80::200:eff:fef1:efa%lan0 icmp_seq=0 hlim=64 time=0.788ms
16 bytes from fe80::200:eff:fef1:efa%lan0 icmp_seq=0 hlim=64 time=0.732ms
16 bytes from fe80::200:eff:fef1:efa%lan0 icmp_seq=0 hlim=64 time=0.715ms
```

第 15 章　表示コマンド

15.1　構成定義の表示

15.1.1　show

[機能]

構成定義情報の表示

[入力形式]

show [<コマンド名>]

[オプション]

なし

[パラメタ]

<コマンド名>

表示したい構成定義のコマンド名を指定します。指定したコマンド名に続く構成定義情報が表示されます。
省略した場合は、すべての構成定義情報が表示されます。

[説明]

構成定義情報を表示します。
未設定時と同じ値が設定されている場合、コマンド名を省略すると表示されません。現在の設定値を表示したい場合にはコマンドも指定します。

[例]

以下に、表示例を示します。

構成定義情報全体を表示する場合

```
# show
wan 0 line isdn
wan 0 isdn limit charge 3000 yes
wan 0 isdn keeptime 2h
lan 0 ip address 192.168.1.1/24 3
lan 0 ip dhcp service server
lan 0 ip dhcp info dns 192.168.1.1
lan 0 ip dhcp info address 192.168.1.2/24 32
lan 0 ip dhcp info time 1d
lan 0 ip dhcp info gateway 192.168.1.1
answer accept disable
answer ppp auth type any
schedule 0 at fri 0000 isdnstat -dramc
syslog pri error,warn,info
syslog facility 23
telnetinfo autologout 5m
time zone 0900
analog dial timer 5
analog hooking timer normal
analog forward on
analog function * on
analog function # mode1
analog ir out ring1
analog ir in ring2
analog ir discrimination ring3
analog numlist add default all
analog priority count 5
tel 1 kind tel
tel 1 global on
tel 1 numbersend net
tel 1 callmode inout
tel 1 volume mid
tel 1 ring herz 20
tel 2 kind tel
tel 2 global on
tel 2 numbersend net
tel 2 callmode inout
tel 2 volume mid
tel 2 ring herz 20
mta service 2
mta timer 10h
#
```

lan 0 インタフェースの IP アド レスを表示する場合

```
# show lan 0 ip address
192.168.1.1/24 3
#
```

15.2 ネットワーク状態の表示

15.2.1 netstat

[機能]

ネットワーク状態の表示

[入力形式]

netstat (ソケット状態表示)
netstat -a (全ソケット状態表示)
netstat -A (PCB アドレスを含んだプロトコル表示)
netstat [-A] [-a] -f <address_family> (指定アドレスファミリソケット状態表示)
netstat -i [-b] [-d] [-I <interface>] (インタフェース統計表示)
netstat -r [-f <address_family>] (ルーティングテーブル表示)
netstat -s [-p <protocol>] (プロトコル統計情報表示)
netstat -r -s [-f <address_family>] (ルーティングテーブル統計情報表示)

[オプション]

-A

ソケットと関係する全プロトコル制御ブロック (PCB) アドレスを含めて、ソケット状態を表示します。

-a

サーバプロセスで利用されているソケットも含めて、すべてのソケットを表示します。なお、通常、サーバプロセスで使用されているソケットは表示されません。

-b

-i と併用して指定する場合に、入出力 byte 数を表示します。

-d

-i と併用して指定する場合に、プロトコル処理部で送信時に欠落したパケット数を合わせて表示します。

-f <address_family>

指定した<address_family>に関する情報だけを表示します。
指定できる<address_family>は、inet(IPv4) と inet6(IPv6) です。
省略した場合は、inet と inet6 の両方を指定したものとみなされます。

-I <interface>

指定した<interface>についての統計情報を表示します。

-i

インタフェース情報を表示します。

-p <protocol>

指定した<protocol>の統計情報を表示します。
指定できる<protocol>は、tcp、udp、ip、icmp、ipsec、tcp6、udp6、ip6、icmp6 です。

-s

各プロトコルの統計情報を表示します。-r と併用して指定する場合は、ルーティングテーブルに関する統計情報を表示します。

-r

ルーティングテーブルを表示します。-s と併用して指定する場合は、ルーティングテーブルに関する統計情報を表示します。

[パラメタ]

なし

[説明]

ソケット状態、ネットワークインタフェース情報、ルーティングテーブル、または統計情報を表示します。

[例]

以下に、表示例および表示内容を示します。

全ソケット状態

```
# netstat -a
Active Internet connections (including servers)
Proto Recv-Q Send-Q  Local Address      Foreign Address      (state)
----- ------ ------  -------------      ---------------      -------
 (1)   (2)    (3)         (4)                (5)              (6)

tcp        0      3  10.232.78.147.23   10.232.77.39.32824   ESTABLISHED
tcp        0      0  *.37               *.0                  LISTEN
tcp        0      0  *.1723             *.0                  LISTEN
tcp        0      0  *.21               *.0                  LISTEN
tcp        0      0  *.80               *.0                  LISTEN
tcp        0      0  *.23               *.0                  LISTEN
udp        0      0  *.0                *.0
udp        0      0  *.37               *.0
udp        0      0  *.520              *.0
udp        0      0  127.0.0.1.7501     *.0
udp        0      0  *.1813             *.0
udp        0      0  127.0.0.1.7500     *.0
udp        0      0  *.1812             *.0
udp        0      0  *.69               *.0
udp        0      0  *.50000            *.0
udp        0      0  *.161              *.0
udp        0      0  *.8900             *.0
udp        0      0  *.53               *.0
udp        0      0  *.123              *.0
udp        0      0  *.67               *.0
udp        0      0  *.0                *.0
udp        0      0  *.59000            *.0
udp        0      0  *.9069             *.0
Active Internet6 connections (including servers)
Proto Recv-Q Send-Q  Local Address      Foreign Address      (state)
tcp6       0      0  *.23               *.0                  LISTEN
udp6       0      0  *.521              *.0
```

1) プロトコル
2) 受信待ち行列長
3) 送信待ち行列長
4) ローカルアドレス
5) リモートアドレス
6) プロトコル内部状態

インタフェース情報表示

```
# netstat -i
Name   Mtu   Network          Address                      Ipkts Ierrs    Opkts Oerrs
---- ---   -------          -------                      ----- -----    ----- -----
(1) (2)(3)     (4)              (5)                        (6)   (7)      (8)   (9)
lan0   1500  <Link#1>         00:00:0e:f1:00:60             487     0       67     0
lan0   1500  10.232.78/24     10.232.78.147                 487     0       67     0
lan0   1500  fe80::/64        fe80::200:eff:fef1:60         487     0        8     0
lo0    16384 <Link#54>                                       0     0        0     0
lo0    16384 fe80::/64        fe80::1                       0     0        0     0
lo0    16384 ::1/128          ::1                           0     0        0     0
lo0    16384 127              127.0.0.1                     0     0        0     0
```

1) 名前
2) ステータス
   名前の後ろに*がついているものは down、それ以外は up です。
3) MTU 長
4) ネットワークおよびサブネットマスク
5) リモートアドレス
6) 入力パケット数
7) 入力エラーパケット数
8) 出力パケット数
9) 出力エラーパケット数

ルーティングテーブル表示

```
# netstat -r
Routing tables

Internet:
Destination              Gateway               Flags      Netif Expire
-----------              -------               -----      ----- ------
   (1)                     (2)                  (3)        (4)   (5)

default                  10.232.78.129         UGSc        lan0
10.232.78/24             link#1                UC          lan0
10.232.78.129            0:a0:c9:78:d8:60      UHLW        lan0   1178
127.0.0.1                127.0.0.1             UH           lo0
Total Routing Tables  0
Total ARP Tables  1

Internet6:
Destination              Gateway               Flags      Netif Expire
::1                      ::1                   UH           lo0
fe80::%lan0/64           link#1                UC          lan0
fe80::%lo0/64            fe80::1%lo0           Uc           lo0
ff01::/32                ::1                   U            lo0
ff02::%lan0/32           link#1                UC          lan0
ff02::%lo0/32            fe80::1%lo0           UC           lo0
Total Routing Tables  0
Total NDP Tables  0
```

1) ネットワークまたはホストの宛先 IP アドレス
2) 宛先ゲートウェイ IP アドレス
3) ルーティング情報を得た手段などを示すフラグ
   フラグの詳細を以下に示します。

   1 ルーティングフラグ#1 にて特定されるプロトコル

   2 ルーティングフラグ#2 にて特定されるプロトコル

3　ルーティングフラグ#3 にて特定されるプロトコル

B　破棄されるパケット

b　ブロードキャストアドレスを表現する経路

C　新しい経路を生成する

c　使用時に、プロトコル専用の新しい経路を生成する

D　リダイレクトによって動的に生成された経路

G　ゲートウェイなどによる中継を必要としている到達先

H　ホストエントリ (これ以外はネットワーク)

L　アドレス変換を連動させられる正当なアドレス

M　リダイレクトによって動的に変更される

R　到達不可能なホストまたはネットワーク

S　スタティックルート

U　使用可能経路

W　クローンした結果として作成された経路

X　外部の daemon がプロトコルからリンクアドレス変換を行う

4)　経由インタフェース

5)　当経路破棄までの残時間 (単位:秒)

統計情報

```
# netstat -s
tcp: ---(1)
        95 packets sent
                90 data packets (16322 bytes)
                0 data packets (0 bytes) retransmitted
                0 resends initiated by MTU discovery
                4 ack-only packets (1 delayed)
                0 URG only packets
                0 window probe packets
                0 window update packets
                1 control packet
        156 packets received
                87 acks (for 16322 bytes)
                1 duplicate ack
                0 acks for unsent data
                72 packets (103 bytes) received in-sequence
                0 completely duplicate packets (0 bytes)
                0 old duplicate packets
                0 packets with some dup. data (0 bytes duped)
                1 out-of-order packet (0 bytes)
                0 packets (0 bytes) of data after window
                0 window probes
                0 window update packets
                0 packets received after close
                0 discarded for bad checksums
                0 discarded for bad header offset fields
                0 discarded because packet too short
        0 connection requests
        2 connection accepts
        0 bad connection attempts
        0 listen queue overflows
        2 connections established (including accepts)
        1 connection closed (including 0 drops)
                1 connection updated cached RTT on close
                1 connection updated cached RTT variance on close
                0 connections updated cached ssthresh on close
        0 embryonic connections dropped
        87 segments updated rtt (of 88 attempts)
        0 retransmit timeouts
                0 connections dropped by rexmit timeout
        0 persist timeouts
                0 connections dropped by persist timeout
        0 keepalive timeouts
                0 keepalive probes sent
                0 connections dropped by keepalive
        76 correct ACK header predictions
        66 correct data packet header predictions

udp: ---(2)
        151 datagrams received
        0 with incomplete header
        0 with bad data length field
        0 with bad checksum
        0 dropped due to no socket
        74 broadcast/multicast datagrams dropped due to no socket
        0 dropped due to full socket buffers
        0 not for hashed pcb
        77 delivered
        0 datagrams output

ip: ---(3)
        307 total packets received
        0 bad header checksums
        0 with size smaller than minimum
        0 with data size < data length
        0 with ip length > max ip packet size
        0 with header length < data size
        0 with data length < header length
        0 with bad options
        0 with incorrect version number
```

(続く)

(続き)

```
        0 fragments received
        0 fragments dropped (dup or out of space)
        0 fragments dropped after timeout
        0 packets reassembled ok
        307 packets for this host
        0 packets for unknown/unsupported protocol
        0 packets forwarded
        0 packets not forwardable
        0 redirects sent
        95 packets sent from this host
        0 packets sent with fabricated ip header
        0 output packets dropped due to no bufs, etc.
        0 output packets discarded due to no route
        0 output datagrams fragmented
        0 fragments created
        0 datagrams that can't be fragmented
        0 tunneling packets that can't find gif

icmp: ---(4)
        0 calls to icmp_error
        0 errors not generated 'cuz old message was icmp
        0 messages with bad code fields
        0 messages < minimum length
        0 bad checksums
        0 messages with bad length
        0 message responses generated

ipsec: ---(5)
        0 inbound packets processed successfully
        0 inbound packets violated process security policy
        0 inbound packets with no SA available
        0 invalid inbound packets
        0 inbound packets failed due to insufficient memory
        0 inbound packets failed getting SPI
        0 inbound packets failed on AH replay check
        0 inbound packets failed on ESP replay check
        0 inbound packets considered authentic
        0 inbound packets failed on authentication
        0 inbound packets considered authentic(ESPinAuth)
        0 inbound packets failed on authentication(ESPinAuth)
        0 outbound packets processed successfully
        0 outbound packets violated process security policy
        0 outbound packets with no SA available
        0 invalid outbound packets
        0 outbound packets failed due to insufficient memory
        0 outbound packets with no route

ip6: ---(6)
        0 total packets received
        0 with size smaller than minimum
        0 with data size < data length
        0 with bad options
        0 with incorrect version number
        0 fragments received
        0 fragments dropped (dup or out of space)
        0 fragments dropped after timeout
        0 fragments that exceeded limit
        0 packets reassembled ok
        0 packets for this host
        0 packets forwarded
        0 packets not forwardable
        0 redirects sent
        6 packets sent from this host
        0 packets sent with fabricated ip header
        0 output packets dropped due to no bufs, etc.
        0 output packets discarded due to no route
        0 output datagrams fragmented
        0 fragments created
        0 datagrams that can't be fragmented
        0 packets that violated scope rules
        0 multicast packets which we don't join
        Mbuf statistics:
                0 one mbuf
```

(続く)

(続き)

```
                0 one ext mbuf
                0 two or more ext mbuf
        0 packets whose headers are not continuous
        0 tunneling packets that can't find gif
        0 packets discarded due to too many headers
        0 failures of source address selection
        0 forward cache hit
        0 forward cache miss

icmp6: ---(7)
        0 calls to icmp6_error
        0 errors not generated because old message was icmp6 error or so
        0 errors not generated because rate limitation
        Output histogram:
                multicast listener report: 5
                neighbor solicitation: 1
        0 messages with bad code fields
        0 messages < minimum length
        0 bad checksums
        0 messages with bad length
        Histogram of error messages to be generated:
                0 no route
                0 administratively prohibited
                0 beyond scope
                0 address unreachable
                0 port unreachable
                0 packet too big
                0 time exceed transit
                0 time exceed reassembly
                0 erroneous header field
                0 unrecognized next header
                0 unrecognized option
                0 redirect
                0 unknown
        0 message responses generated
        0 messages with too many ND options

tcp6: ---(8)
        0 packets sent
                0 data packets (0 bytes)
                0 data packets (0 bytes) retransmitted
                0 ack-only packets (0 delayed)
                0 URG only packets
                0 window probe packets
                0 window update packets
                0 control packets
        0 packets received
                0 acks (for 0 bytes)
                0 duplicate acks
                0 acks for unsent data
                0 packets (0 bytes) received in-sequence
                0 completely duplicate packets (0 bytes)
                0 old duplicate packets
                0 packets with some dup. data (0 bytes duped)
                0 out-of-order packets (0 bytes)
                0 packets (0 bytes) of data after window
                0 window probes
                0 window update packets
                0 packets received after close
                0 discarded for bad checksums
                0 discarded for bad header offset fields
                0 discarded because packet too short
        0 connection requests
        0 connection accepts
        0 bad connection attempts
        0 connections established (including accepts)
        0 connections closed (including 0 drops)
        0 embryonic connections dropped
        0 segments updated rtt (of 0 attempts)
        0 retransmit timeouts
```

(続く)

(続き)

```
                0 connections dropped by rexmit timeout
        0 persist timeouts
        0 connections timed out in persist
        0 keepalive timeouts
                0 keepalive probes sent
                0 connections dropped by keepalive
        0 correct ACK header predictions
        0 correct data packet header predictions
        0 PCB cache misses

udp6: ---(9)
        0 datagrams received
        0 with incomplete header
        0 with bad data length field
        0 with bad checksum
        0 with no checksum
        0 dropped due to no socket
        0 multicast datagrams dropped due to no socket
        0 dropped due to full socket buffers
        0 delivered
        0 datagrams output
```

1) TCP 統計情報
2) UDP 統計情報
3) IP 統計情報
4) ICMP 統計情報
5) IPSEC 統計情報
6) IP6 統計情報
7) ICMP6 統計情報
8) TCP6 統計情報
9) UDP6 統計情報

15.2.2 dhcpstat

[機能]

DHCP 運用状況の表示

[入力形式]

dhcpstat [<interface>]

[オプション]

なし

[パラメタ]

<interface>

- LAN インタフェース番号
  LAN インタフェース番号として、0 を指定してください。
  省略した場合は、 DHCP が動作可能なインタフェースすべてを指定したものとみなされます。
  指定した LAN インタフェース番号で DHCP サーバ、DHCP リレーエージェントのいずれも動作していない場合は、何も表示されません。

[説明]

DHCP の以下の機能の運用状況を表示します。

- DHCP サーバ機能
  リース可能アドレスレンジ、リース中のアドレス、リース先情報、およびリース期間を表示します。
- DHCP リレーエージェント機能
  中継先 DHCP サーバのアドレスを表示します。

[例]

以下に、表示例を示します。

DHCP サーバの場合

```
# dhcpstat 0

[LAN0] DHCP Server Informations

Lease IP Address          : 192.168.1.2  [Range: 253]
Subnet Mask               : 255.255.255.0
DNS Server Address        : 0.0.0.0, 0.0.0.0
Lease Time                : 0001.00:00:00
Default Router Address    : 192.168.1.1
Domain Name               : pfu.co.jp

Active Client List:
No. IP address          MAC address       Lease remain
001 192.168.1.2         00:00:00:00:00:00 0000.23:59:00
002 192.168.1.3         00:00:00:00:00:00 0000.23:59:00
003 192.168.1.4         00:00:00:00:00:00 0000.23:59:00
004 192.168.1.5         00:00:00:00:00:00 0000.23:59:00
005 192.168.1.6         00:00:00:00:00:00 0000.23:59:00
:

#
```

DHCP リレーエージェント の場合

```
# dhcpstat 0
[LAN0] DHCP Relay Agent Information
Forwarding DHCP Server: 192.168.3.1
#
```

15.2.3 routestat

[機能]

IPv4 ルーティング情報 (経路情報) の表示

[入力形式]

routestat ip_route (経路情報表示)
routestat ip_rip (RIP 経路情報表示)
routestat ip_protocols_rip (RIP プロトコル情報表示)
routestat ip_bgp (BGP 経路情報表示)
routestat ip_bgp_neighbors (BGP 相手装置情報表示)
routestat ip_all (全情報表示)

[オプション]

なし

[パラメタ]

ip_route
保持している経路情報を表示します。

ip_rip
RIP 経路に関連した情報を表示します。

ip_protocols_rip
RIP プロトコルに関連した情報を表示します。

ip_bgp
BGP 経路に関連した情報を表示します。

ip_bgp_neighbors
BGP 相手装置に関連した情報を表示します。

ip_all
上記の情報をすべて表示します。

[説明]

IPv4 ルーティング情報 (経路情報) を表示します。

[例]

以下に、表示例および表示内容を示します。

保持している経路情報表示の場合

```
# routestat ip_route
Codes: C - connected, S - static, R - RIP, B - BGP,
       > - selected route, * - FIB route

C> * 192.168.10.0/24 is directly connected, lan0
C> * 192.168.30.1/32 is directly connected, rmt0
C> * 192.168.30.2/32 is directly connected, rmt0
R> * 192.168.80.0/24 [120/2] via 192.168.10.50, lan0, 00:11:35
R> * 192.168.81.0/24 [120/3] via 192.168.10.50, lan0, 00:11:35
R> * 192.168.82.0/24 [120/3] via 192.168.10.50, lan0, 00:11:34
(1)     (2)          (3)       (4)           (5)    (6)
```

1) ルーティングプロトコル種別 (Codes)
以下のいずれかが表示されます。

C :　インタフェース経路

S :　スタティック経路

R :　RIP 経路

B :　BGP 経路

> :　同一経路の中で優先される経路

*** :**　IP ルーティングで使用される有効経路

2) 経路のネットワークアドレス/マスクビット数
インタフェース経路で、かつ、remote 側に IP アドレスが割り振られていない場合、"unnumbered"が表示されます。デフォルトルート (0.0.0.0/0) の場合は、"default"が表示されます。

3) 優先度/メトリック値 ([distance/metric])
インタフェース経路のときは表示されません。

4) 経路情報送信元 IPv4 アドレス
以下のいずれかが表示されます。

"**via IPv4address**"
送信元の IPv4 アドレスが表示されます。

"**is directly connected**"
インタフェース経路、または、送信元 IPv4 アドレスが存在しないスタティック経路のときに表示されます。

5) インタフェース名
インタフェースを表示します。状態により以下のいずれかが表示される場合があります。

"**inactive**"
使用不可能状態

"**(recursive via IPv4address)**"
BGP 使用時、リカーシブ (経由ネットワークとして IPv4 アドレスを使用) の場合に表示されます。

"**(recursive is directly connected)**"
BGP 使用時、リカーシブ (経由ネットワークとしてインタフェース経路を使用) の場合に表示されます。

6) 時間
経路情報を更新してから経過した時間が表示されます。
RIP 経路または BGP 経路の場合に表示されます。

RIP 経路情報表示の場合

```
# routestat ip_rip
Codes: R - RIP, C - connected, S - static, B - BGP

   Network            Next Hop         Metric From            Time
(1)   (2)               (3)             (4)    (5)             (6)
B  11.11.10.0/24      192.168.10.30         1
B  40.40.40.0/24      192.168.10.30         1
C  192.168.10.0/24                          1
C  192.168.20.0/24                          1
S  192.168.22.0/24    192.168.10.11        11
S  192.168.30.0/24    192.168.10.11         2
R  192.168.31.0/24    192.168.10.10         3 192.168.10.10   02:49
R  192.168.32.0/24    192.168.10.10         7 192.168.10.10   02:49
R  192.168.80.0/24    192.168.10.50         2 192.168.10.50   02:55
S  192.168.81.0/24    192.168.10.11         2
R  192.168.82.0/24    192.168.10.50         3 192.168.10.50   02:55
S  192.168.100.0/24   192.168.10.11         6
```

1) ルーティングプロトコル種別 (Codes)
   以下のいずれかが表示されます。

   C : インタフェース経路

   B : BGP 経路

   R : RIP 経路

   S : スタティック経路

2) 経路のネットワークアドレス/マスクビット数 (Network)
   インタフェース経路で、かつ、remote 側に IP アドレスが割り振られていない場合、"unnumbered"が表示されます。デフォルトルート (0.0.0.0/0) の場合は、"default"が表示されます。

3) ネクストホップルータの IP アドレス (Next Hop)

4) メトリック値 (Metric)
   このメトリック値がネットワーク上に広報されます。
   ただし、加算メトリックが設定されている場合は、この Metric 値+加算メトリック値が広報されます。

5) 送信元 IPv4 アドレス (From)
   RIP 経路の場合、送信元 IPv4 アドレスが表示されます。

6) 時間 (Time)
   タイムアウトされるまでの時間を表示します。初期値は、3:00(分) であり、0:00 になると、この経路に関しては、メトリック値が 16 で広報されることを意味します。

RIP プロトコル情報表示の場合

```
#routestat ip_protocols_rip
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50%, next due in 24 seconds   (1)
  Timeout after 180 seconds, garbage collect after 120 seconds           (2)
  Default redistribution metric is 1                                      (3)
  Redistributing:                                                         (4)
    redistribute static
    redistribute connected
    redistribute bgp metric 5
  Routing network:                                                        (5)
    Interface        Send  Recv   Add-Metric  Ignore  Passwd
    lan0             v2m   v2             0     off
    rmt0             v2m   v2             5     off
  Routing Information Sources:
    Gateway          BadPackets BadRoutes  Distance Last Update          (6)
    192.168.10.10            0         0       120   00:00:07
    192.168.30.10            0         0       120   00:00:24
    192.168.10.50            0         0       120   00:00:13
  Distance: (default is 120)                                              (7)
```

1) Sending updates every 30 seconds with +/-50%, next due in 24 seconds
   RIP 定期広報に関する情報を表示します。
   RIP 定期広報は、30 秒間隔 (15 秒のゆらぎ) で行われており、次の広報時間を表示します。(この表示例の場合は、約 24 秒後です。)

2) Timeout after 180 seconds, garbage collect after 120 seconds
   RIP のタイムアウトに関する情報を表示します。
   RIP タイムアウト時間は、180 秒であり、ガーベージタイマーは、120 秒であることを意味します。

3) Default redistribution metric is 1
   再広報する経路種別に対するメトリックは、1 加算して処理することを意味します。

4) Redistributing:
   再広報を対象とするプロトコルに関する情報を表示します。

5) Routing network:
自装置側で設定されている RIP の構成定義に関する情報を表示します。

Interface :
構成定義で設定したインタフェース名

Send : 送信モードを表示します。

Off : RIP パケットを送信しない

v1 : RIPv1 で送信

v2 : RIPv2(ブロードキャスト) で送信

v2m : RIPv2(マルチキャスト) で送信

Recv : 受信モードを表示します。

Off : RIP パケットを受信しない

v1 : RIPv1 のみ受信

v2 : RIPv1,RIPv2(ブロードキャスト / マルチキャスト) で受信

Add-Metric:
加算メトリック値を表示します。

Ignore : RIPv2 認証つきパケットを受信した場合の動作

Off : RIPv2 パケットを受信した場合、破棄しません。

On : RIPv2 パケットを受信した場合、破棄します。

Passwd : RIPv2 で認証機能を使用する場合のパスワードを表示します。

6) Routing Information Sources:
RIP の通信を行っている相手ルータの情報を表示します。

Gateway :
相手ルータの IP アドレスを表示します。

BadPackets:
RIP パケット内の異常パケット数の累積数を表示します。

BadRoutes :
RIP パケット内の経路情報に関する異常経路数の累積数を表示します。

Distance :
相手ルータの優先度を表示します。現状は 120 固定で表示されます。

Update : 相手ルータとの接続時間を表示します。

7) Distance:
自装置の RIP の優先度を表示します。

BGP 経路情報表示の場合

```
# routestat ip_bgp
BGP local router ID is 192.168.40.2
Status codes: s suppressed, * valid, > best
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric Path
(1)  (2)              (3)                (4)    (5)  (6)
*> 20.0.0.0         0.0.0.0                       i
*> 30.30.30.0/24    172.16.10.30                  ?
*> 50.50.50.0/24    192.168.1.20             50 65000 i
*> 172.16.10.0/24   0.0.0.0                       ?
*> 172.16.20.0/24   0.0.0.0                       ?
*> 192.168.1.10/32  0.0.0.0                       ?
*> 192.168.1.20/32  0.0.0.0                       ?

Total number of prefixes 7
```

1) 状態 (Status)
   以下のいずれかが表示されます。

   s : 他経路に集約されている経路

   *** :** 有効経路

   > : ベストパス

2) 経路のネットワークアドレス/マスクビット数 (Network)
   デフォルトルートの場合は 0.0.0.0/0 と表示されます。

3) ネクストホップ (Next Hop)
   bgp network コマンドで設定した経路やインタフェース経路は 0.0.0.0 と表示されます。

4) メトリック値 (Metric)

5) パス (Path)
   経由した AS 番号が表示されます。自装置が属する AS が広報の起点の場合は表示されません。

6) オリジン (Origin)
   以下のいずれかが表示されます。なお、Path の表示がない場合、Path の位置に表示されます。

   i : AS 内部で生成した経路

   e : EGP を通して受信した経路

   ? : BGP で学習したスタティク経路およびインタフェース経路

BGP の機能が動作していないときは、以下が表示されます。

```
# routestat ip_bgp
No BGP process is configured
```

BGP の機能を開始中や経路情報がない場合は以下が表示されます。

```
# routestat ip_bgp
No BGP network exists
```

BGP 相手装置情報表示の場合

```
# routestat ip_bgp_neighbors
BGP neighbor is 192.168.40.1, remote AS 1234, local AS 5678, external link (1)
  BGP version 4, remote router ID 192.168.40.1                               (2)
  BGP state = Established, up for 00:00:24                                   (3)
  Last read 00:00:23, hold time is 90, keepalive interval is 30 seconds      (4)
  Configured hold time is 90, keepalive interval is 30 seconds               (5)
  Neighbor capabilities:                                                     (6)
    Route refresh: advertised and received(old)
    Address family IPv4 Unicast: advertised and received
  Received 3 messages, 0 notifications, 0 in queue                           (7)
  Sent 4 messages, 0 notifications, 0 in queue                               (8)
  Route refresh request: received 0, sent 0                                  (9)

 For address family: IPv4 Unicast                                           (10)
  NEXT_HOP is always this router                                            (11)
  1 accepted prefixes                                                       (12)
  2 announced prefixes                                                      (13)

  Connections established 1; dropped 0                                      (14)
Local host: 192.168.40.2, Local port: 1038                                  (15)
Foreign host: 192.168.40.1, Foreign port: 179                               (16)
Nexthop: 192.168.40.2                                                       (17)
Read thread: on  Write thread: off                                          (18)
```

1) BGP neighbor is 192.168.40.1, remote AS 1234, local AS 5678, external link
相手装置の IP アドレス、相手装置の属する AS 番号, 自装置の属する AS 番号を示します。
"external link"は BGP 接続形態が EBGP であることを示します。

2) BGP version 4, remote router ID 192.168.40.1
自装置の BGP 版数と相手装置の router-ID を示します。

3) BGP state = Established, up for 00:00:24
BGP 状態と BGP 接続が確立してからの経過時間を示します。
BGP 状態には以下があります。

Idle :　アイドル状態

Connect :
接続中状態

Active :　アクティブ状態

OpenSent :
OPEN メッセージ待ち状態

OpenConfirm:
BGP 接続確立のための KEEPALIVE メッセージ待ち状態

Established:
BGP 接続が確立した状態

4) Last read 00:00:23, hold time is 90, keepalive interval is 30 seconds
相手装置から最後にメッセージ受信してからの経過時間、Holdtime タイマの値、Keepalive タイマの値を示します。

5) Configured hold time is 90, keepalive interval is 30 seconds
自装置での Holdtime タイマの設定値、自装置での Keepalive タイマの設定値を示します。

6) Neighbor capabilities:
相手装置とネゴシエートしたケイパビリティを以下の情報で表示します。

- Route refresh: advertised and received(old)
  Route refresh capability(OLD) を示します。
- Address family IPv4 Unicast: advertised and received
  Multiprotocol extension capability(IPv4 unicast) を示します。

7) Received 3 messages, 0 notifications, 0 in queue
受信したメッセージ数、受信した NOTIFICATION 数、未処理の受信メッセージ数を示します。

8) Sent 4 messages, 0 notifications, 0 in queue
送信したメッセージ数、送信した NOTIFICATION 数、未処理の送信メッセージ数を示します。

9) Route refresh request: received 0, sent 0
ROUTE_REFRESH メッセージの送受信メッセージ数を示します。

10) For address family: IPv4 Unicast
使用するアドレスファミリが IPv4 Unicast であることを示します。

11) NEXT_HOP is always this router
NEXTHOP を常に自装置のアドレスとして広報することを示します。

12) 1 accepted prefixes
相手装置から受信した経路情報の数を示します。

13) 2 announced prefixes
自装置から広報した経路情報の数を示します。

14) Connections established 1; dropped 0
Established 状態となった回数、および、Established 状態で BGP 接続を終了した回数を示します。

15) Local host: 192.168.40.2, Local port: 1038
BGP 接続に使用している自装置の IP アドレスとポート番号を示します。

16) Foreign host: 192.168.40.1, Foreign port: 179
BGP 接続に使用している相手装置の IP アドレスとポート番号を示します。

17) Nexthop: 192.168.40.2
NEXTHOP として使用する IP アドレスを示します。

18) Read thread: on Write thread: off
受信 / 送信処理状況を示します。
受信可能状態の場合は "Read thread: on"が表示され、受信不可状態の場合は"Read thread: off"が表示されます。
送信処理中の場合は "Write thread: on"が表示され、送信処理を行っていない場合は "Write thread: off"が表示されます。

15.3　回線状態の表示

15.3.1　lineis

[機能]

回線の状態表示

[入力形式]

lineis

[オプション]

なし

[パラメタ]

なし

[説明]

WAN 回線の接続状況を表示します。

[例]

以下に、各回線種別の表示例および表示内容を示します。

回線種別が専用線の場合

```
# lineis
line type               : HSD 64Kbps                    --- (1)
line status             : connected                     --- (2)
communicated time       : 0000.00:30:03                 --- (3)
IPCP                    : opened                        --- (4)
negotiated IP address   : 192.168.1.1 -> 192.168.2.1    --- (5)
IPV6CP                  : opened                        --- (6)
BCP                     : opened                        --- (7)
```

1)　回線種別

以下のいずれかが表示されます。

HSD 64Kbps

専用線 (64Kbps)

HSD 128Kbps

専用線 (128Kbps)

2)　回線状態

以下のいずれかが表示されます。

enabling　同期確立中

synchronization failed

同期はずれ状態

connected

通信中

idle　回線未使用

3) 通信時間

「line status」が connected の場合にだけ、dddd.hh:mm:ss の形式で通信時間が表示されます。dddd=日数、hh=時間、mm=分、ss=秒を示します。

4) IPCP 状態

「line status」が connected の場合にだけ、以下のいずれかが表示されます。

opened IPv4 利用可能

negotiating
IPCP ネゴシエーション中

closed IPv4 利用不可能

5) 自側 IP アドレス→相手側 IP アドレス

「line status」が connected の場合にだけ、IPCP のアドレスネゴシエーション結果が表示されます。アドレスネゴシエーションなしで接続した場合は、255.255.255.255 となります。

6) IPV6CP 状態

「line status」が connected の場合にだけ、以下のいずれかが表示されます。

opened IPv6 利用可能

negotiating
IPv6CP ネゴシエーション中

closed IPv6 利用不可能

7) BCP 状態

「line status」が connected の場合にだけ、以下のいずれかが表示されます。

opened Bridge 利用可能

negotiating
BCP ネゴシエーション中

closed Bridge 利用不可能

回線種別が ISDN 回線の場合

```
# lineis
line type             : ISDN                              --- (1)
dial no 0             : *                                 --- (2)
dial no 1             : *                                 --- (3)
<B1ch>
channel status        : connected(MP)                     --- (4)
call status           : call-out                          --- (5)
remote target         : tokyo.ap1 [remote 0 ap 0]         --- (6)
remote TEL no         : 4588*                             --- (7)
line speed            : 64000 bps                         --- (8)
communicated time     : 0000.00:00:01                     --- (9)
IPCP                  : opened                            --- (10)
negotiated IP address : 192.168.1.1 -> 255.255.255.255    --- (11)
DNS server address    : 255.255.255.255                   --- (12)
IPV6CP                : opened                            --- (13)
BCP                   : opened                            --- (14)
send/receive traffic  : 0%/0%                             --- (15)
<B2ch>
channel status        : connected(MP)                     --- (4)
call status           : call-out                          --- (5)
remote target         :  [remote 0 ap 0]                  --- (6)
remote TEL no         : 4588*                             --- (7)
line speed            : 64000 bps                         --- (8)
communicated time     : 0000.00:00:04                     --- (9)
IPCP                  : opened                            --- (10)
negotiated IP address : 192.168.1.1 -> 255.255.255.255    --- (11)
DNS server address    : 255.255.255.255                   --- (12)
IPV6CP                : opened                            --- (13)
BCP                   : opened                            --- (14)
send/receive traffic  : 0%/0%                             --- (15)
```

1) 回線種別
ISDN(ISDN 回線利用中) が表示されます。

2) 自局番号 0
設定済みの自局番号 0 が表示されます。「*」以降はサブアドレスです。

3) 自局番号 1
設定済みの自局番号 1 が表示されます。「*」以降はサブアドレスです。

4) 回線状態
以下のいずれかが表示されます。

enabling　同期確立中

synchronization failed
同期はずれ状態

idle　チャネル未使用

disconnecting
切断中

connected
通信中

connected(MP)
MP で通信中

callin　着信処理中

alerting　相手呼出中

5) 接続方向
「channel status」が connected の場合にだけ、以下のいずれかが表示されます。

call-out　発信によって接続

call-in　着信によって接続

6) ネットワーク名、接続先名
「channel status」が connected の場合にだけ、接続先が表示されます。

7) 接続先電話番号
「channel status」が connected の場合にだけ、接続先の電話番号が表示されます。

8) 回線速度
「channel status」が connected の場合にだけ、接続中の回線の回線速度が表示されます。

9) 通信時間
「channel status」が connected の場合にだけ、dddd.hh:mm:ss の形式で通信時間が表示されます。
dddd=日数、hh=時間、mm=分、ss=秒を示します。

10) IPCP 状態
「channel status」が connected の場合にだけ、以下のいずれかが表示されます。

opened　IPv4 利用可能

negotiating
IPCP ネゴシエーション中

closed　IPv4 利用不可能

11) 自側 IP アドレス→相手側 IP アドレス

「channel status」が connected の場合にだけ、IPCP のアドレスネゴシエーション結果が表示されます。アドレスネゴシエーションなしで接続した場合は、255.255.255.255 となります。

12) DNS サーバアドレス

IPCP が enable の場合に DNS サーバアドレスネゴシエーション結果が表示されます。DNS サーバアドレスネゴシエーションなしで接続した場合には 255.255.255.255 となります。

13) IPV6CP 状態

「channel status」が connected の場合にだけ、以下のいずれかが表示されます。

opened IPv6 利用可能

negotiating

IPv6CP ネゴシエーション中

closed IPv6 利用不可能

14) BCP 状態

「channel status」が connected の場合にだけ、以下のいずれかが表示されます。

opened Bridge 利用可能

negotiating

BCP ネゴシエーション中

closed Bridge 利用不可能

15) 送信回線使用率 / 受信回線使用率

「channel status」が connected の場合にだけ、データ送受信における回線使用率が表示されます。

回線種別がフレームリレーの場合

```
# lineis
line type             : FR 128Kbps                    ---(1)

<DLCI: 17>
channel status        : synchronization failed        ---(2)
communicated time     : 0000.00:00:00                 ---(3)
remote target         : rmt0.ap0 [remote 0 ap 0]      ---(4)
remote DLCI           : 0                             ---(5)
remote IP address     : 192.168.100.2                 ---(6)
local IP address      : 192.168.100.1                 ---(7)
CIR                   : 0                             ---(8)
send/receive traffic  : 0%/0%                         ---(9)
```

1) 回線種別

以下のいずれかが表示されます。

FR 64Kbps

フレームリレー (64Kbps)

FR 128Kbps

フレームリレー (128Kbps)

2) チャネル状態

以下のいずれかが表示されます。

enabling 同期確立中

synchronization failed

同期はずれ状態

connected

通信中

3) 通信時間

dddd.hh:mm:ss の形式で通信時間が表示されます。dddd=日数、hh=時間、mm=分、ss=秒を示します。

4) ネットワーク名

相手ネットワーク名が表示されます。

5) 相手 DLCI

相手 DLCI が表示されます。

6) 相手 IP アドレス

相手 IP アドレスが表示されます。

7) 自 IP アドレス

自 IP アドレスが表示されます。

8) CIR

定義した CIR(認定情報速度) が表示されます。

9) 送信回線使用率 / 受信回線使用率

データ送受信における回線使用率が表示されます。

15.3.2 isdnstat

[機能]

ISDN 関連の統計情報の表示

[入力形式]

isdnstat -{D | d | r | m | a | c}

[オプション]

-D

データ通信の発着信統計情報を一覧表示します。以下の情報が表示されます。

- 発信回数
- 相手ビジーによる発信失敗回数
- ほかの網理由によるエラーによる発信失敗回数
- 着信回数
- 着信拒否回数

-d

データ通信としての課金および時間の統計情報を一覧表示します。以下の情報が表示されます。

- 発信での通信総時間
- 総課金
- 1 回あたりの最長時間、そのときの課金、および接続先
- 1 回あたりの最高課金、そのときの時間、および接続先
- 最終接続の時間、課金、および接続先

-r

課金および時間の統計情報を一覧表示します。以下の情報が表示されます。

- 接続アクセスポイントごとの、通信総時間および総課金

-a

アナログ通信としての課金および時間の統計情報を一覧表示します。以下の情報が表示されます。

- 発信での通信総時間
- 総課金合計
- 1 回あたりの最長時間、およびそのときの課金、接続先電話番号
- 1 回あたりの最高課金、およびそのときの時間、接続先電話番号
- 最終接続の時間、課金、接続先

-m

マルチ TA 通信としての課金および時間の統計情報を一覧表示します。以下の情報が表示されます。

- 発信での通話総時間
- 総課金合計

-c

課金情報をクリアします。対象となるデータを表示するオプションと同時に表示します。

[パラメタ]

なし

[説明]

ISDN 接続関連の統計情報を表示します。
発信には、自身の要求による発信だけではなく、コールバック応答としての発信も含まれます。

[例]

以下に、各オプションの表示例および表示内容を示します。

発着信統計情報を表示する場合 (-D 指定時)

```
# isdnstat -D
[wan 0]
call setup count        = 2  --- (1)
call busy count         = 0  --- (2)
call error count        = 0  --- (3)
called accept count     = 0  --- (4)
called reject count     = 0  --- (5)
```

1) 発信の回数
2) 着ユーザビジーによって発信失敗した回数
3) 着ユーザビジー以外の網理由で発信失敗した回数
4) 着信の回数
5) 着信を拒否した回数

課金統計情報を表示する場合 (-d 指定時)

```
# isdnstat -d
[wan 0]
total time for callout  = 0000.00:03:04      --- (1)
total charge            = 10                 --- (2)
peek time   remote      = internet.ISP-1     --- (3)
            time        = 0000.00:02:57      --- (4)
            charge      = 10                 --- (5)
peek charge remote      = internet.ISP-1     --- (6)
            time        = 0000.00:02:57      --- (7)
            charge      = 10                 --- (8)
last        remote      = intranet.OFFICE-I  --- (9)
            time        = 0000.00:00:07      --- (10)
            charge      = 0                  --- (11)
```

1) 発信接続の総通信時間
2) 総課金額
3) 最長接続時の相手名
4) 最長接続時の接続時間
5) 最長接続時の課金額
6) 最高課金時の相手名
7) 最高課金時の接続時間
8) 最高課金時の課金額
9) 最終接続時の相手名
10) 最終接続時の接続時間
11) 最終接続時の課金額

相手ごとのデータ通信課金統計情報を表示する場合 (-r 指定時)

```
# isdnstat -r
remote  ap    charge  time
------  --    ------  ----
 (1)    (2)    (3)     (4)

     0   0        10  0000.00:02:57
     1   0         0  0000.00:00:07
```

1) 相手定義番号
2) アクセスポイント定義番号
3) 課金の合計金額
4) 接続の合計時間

アナログ通信課金統計情報を表示する場合 (-a 指定)

```
# isdnstat -a
total time for callout  = 0000.00:05:12  --- (1)
total charge            = 30             --- (2)
peek time   dial No.    = 0123456789     --- (3)
            time        = 0000.00:04:11  --- (4)
            charge      = 20             --- (5)
peek charge dial No.    = 0123456789     --- (6)
            time        = 0000.00:04:11  --- (7)
            charge      = 20             --- (8)
last        dial No.    = 0123459876     --- (9)
            time        = 0000.00:01:01  --- (10)
            charge      = 10             --- (11)
```

1) 発信接続の総通信時間
2) 総課金額
3) 最長接続時の相手電話番号
4) 最長接続時の接続時間
5) 最長接続時の課金額
6) 最高課金時の相手電話番号
7) 最高課金時の接続時間
8) 最高課金時の課金額
9) 最終接続時の相手電話番号
10) 最終接続時の接続時間
11) 最終接続時の課金額

マルチ TA 通信課金統計情報を表示する場合 (-m 指定時)

```
# isdnstat -m
total time for callout  = 0000.00:06:12  --- (1)
total charge            = 30             --- (2)
```

1) 発信接続の総通信時間
2) 総課金額

15.3.3　frstat

[機能]

フレームリレーの PVC 状態、および統計情報の表示

[入力形式]

frstat [<dlci>]

[オプション]

なし

[パラメタ]

<dlci>

- DLCI 番号
  表示する DLCI の番号を、16～991 の 10 進数値で指定します。
  省略した場合は、すべての DLCI を指定したものとみなされます。

[説明]

フレームリレーの PVC 状態および統計情報を表示します。

[例]

以下に、表示例を示します。

```
# frstat

[DLCI: 16]
  CIR                   : 0
  trans state           : active
  load state            : send(min)
  possible send bytes   : 819
  max send bytes        : 819
  max send bytes(lower) : 819
  max send bytes(upper) : 819
  max send bytes(CIR)   : 819
  sending bytes         : 0
  send throughput       : 0 bytes/s
  waiting send packets  : 0
  fecn received         : 0
  becn received         : 0
  send errors           : 0
  receive errors        : 0
  send bytes            : 37141
  receive bytes         : 1426753

[DLCI: 17]
  CIR                   : 0
  trans state           : active
  load state            : send(min)
  possible send bytes   : 819
  max send bytes        : 819
  max send bytes(lower) : 819
  max send bytes(upper) : 819
  max send bytes(CIR)   : 819
  sending bytes         : 0
  send throughput       : 0 bytes/s
  waiting send packets  : 0
  fecn received         : 0
  becn received         : 0
  send errors           : 0
  receive errors        : 0
  send bytes            : 0
  receive bytes         : 0

#
```

以下に表示内容を示します。

```
DLCI                    : DLCI番号
CIR                     : CIR値
trans state             : 伝送制御現状態

                          ・disable       enable指示待ち
                          ・inactive      enable状態(inactive)
                          ・active        enable状態(active)

load state              : 輻輳制御現状態

                          ・stop                  停止状態
                          ・send(min)             下限値で送信中
                          ・send(min..cir)        下限からCIRで送信中
                          ・send(cir)             CIRで送信中
                          ・send(cir..max)        CIRから上限で送信中
                          ・send(max)             上限値で送信中

possible send bytes     : 送出可能データ量(byte)
max send bytes          : Tc(100ms)時間内に送出できる最大データ長(byte)
max send bytes(lower)   : Tc(100ms)時間内に送出できる最大データ長の下限値(byte)
max send bytes(upper)   : Tc(100ms)時間内に送出できる最大データ長の上限値(byte)
max send bytes(CIR)     : Tc(100ms)時間内に送出できる最大データ長にCIR値適用(byte)
sending bytes           : 送信中バイト数（残り）
send throuput           : 送信スループット(byte/s)
waiting send packets    : 送信待ちパケット数
fecn received           : 1時間ごとのFECN ONフレーム受信回数
becn received           : 1時間ごとのBECN ONフレーム受信回数
send errors             : 送信フレーム破棄回数（合計）
receive errors          : 受信フレーム破棄回数（合計）
send bytes              : 送信バイト数（合計）
receive bytes           : 受信バイト数（合計）
```

15.4　統計情報の表示

15.4.1　stlan

[機能]

LAN ドライバの統計情報の表示

[入力形式]

stlan

[オプション]

なし

[パラメタ]

なし

[説明]

LAN ドライバの統計情報を表示します。

[注意]

統計情報は、本装置を再起動するとクリアされます。

[例]

以下に、表示例および表示内容を示します。

```
# stlan

[LAN STATUS]
driver stage              : init     --- (1)
[LAN LOG INFORMATION]
Input packets             : 2      --- (3)
Input error packets       : 65537  --- (4)
 long frame               : 0      --- (5)
 bad alignment frame      : 0      --- (6)
 short frame              : 0      --- (7)
 CRC error                : 0      --- (8)
 overrun                  : 0      --- (9)
 late collision           : 0      --- (10)
Output packets            : 65537  --- (11)
Output error packets      : 0      --- (12)
 late collision           : 0      --- (13)
 too many collision       : 0      --- (14)
 underrun                 : 0      --- (15)
 loss of carrier          : 0      --- (16)
```

1) driver stage

3) 受信フレーム数

4) 受信エラーフレーム数

5) 最大フレーム長オーバ検出回数

6) アライメントエラー検出回数

7) ショートフレーム検出回数

8) CRC エラー検出回数

9) オーバーラン検出回数
10) レイトコリジョン検出回数
11) 送信フレーム数
12) 送信エラーフレーム数
13) レイトコリジョン検出回数
14) コリジョン発生による送信リトライアウト検出回数
15) アンダーラン検出回数
16) キャリアセンスロスト検出回数

15.4.2　stins

[機能]

ISDN 統計情報の表示

[入力形式]

stins [<channel>]

[オプション]

なし

[パラメタ]

<channel>

チャネル番号

- d
  Dch
- b1
  B1ch
- b2
  B2ch

[説明]

ISDN 統計情報を表示します。
<channel>を省略した場合は、d,b1,b2 の順に全チャネルの情報を表示します。

[注意]

統計情報は再起動によりクリアされます。

[例]

以下に表示例および表示内容を示します。

ISDN 表示例

```
# stins d
[LINE STATUS]
date                    : Jan 14 17:25:32 2003  --- (1)
type                    : isdn                  --- (2)
channel                 : [D]                   --- (3)
 speed                  : 16k                   --- (4)
 status                 : wait sync             --- (5)
 since                  : Jan 14 17:09:09 2003  --- (6)
 func                   : Q921                  --- (7)
[LINE LOG INFORMATION]
received frame          : 0                     --- (8)
sent frame              : 0                     --- (9)
Input frame dropped
  busy                  : 0                     --- (10)
  DPLL error            : 0                     --- (11)
  CD lost               : 0                     --- (12)
  overrun               : 0                     --- (13)
  CRC error             : 0                     --- (14)
  abort frame           : 0                     --- (15)
  bad length            : 0                     --- (16)
  bad octet             : 0                     --- (17)
Output frame dropped
  underrun              : 0                     --- (18)
  CTS lost              : 0                     --- (19)
```

表示内容の説明 (D/B チャネル表示)

1) コマンド 投入時刻

   stins コマンド が入力された時刻を表示します。

2) 回線種別

   - isdn: ISDN
   - hsd : 専用線
   - fr : フレームリレー

3) チャネル種別

   - D
   - B1
   - B2

4) 通信速度

   - 16k
   - 32k
   - 64k
   - 128k

5) チャネル状態

   - init : 初期化中状態
   - wait setline : チャネル未使用状態
   - wait enable : イネーブル待ち状態
   - wait sync : 同期確立待ち状態
   - outsync : 同期はずれ検出中状態
   - data : データ送受信可能状態

6) 状態遷移時刻
   チャネル状態が現在の状態に変化した時刻を表示します。
7) 通信手順
   D チャネルの場合
   - Q921

   B チャネルの場合
   - HDLC
   - PIAFS (PIAFS 通信使用中)

   以下の情報は、B1/B2 チャネルにおいて PIAFS 通信時にはカウントアップされません。
8) 受信フレーム数
9) 送信フレーム数
10) 受信バッファビジー検出回数
11) 受信 DPLL エラー検出回数
12) 受信キャリア消失検出回数
13) 受信オーバーラン検出回数
14) 受信 CRC エラー検出回数
15) 受信アボートエラー検出回数
16) 受信フレーム長違反検出回数
17) 受信非オクテットフレーム検出回数
18) 送信アンダーラン検出回数
19) 送信 CTS 消失検出回数

15.4.3 bridgestat

[機能]

ブリッジに関する状態および統計情報の表示

[入力形式]

bridgestat -i [-I <interface>] (入出力パケット数表示)
bridgestat -l [-I <interface>] (学習テーブル情報表示)
bridgestat -t (学習テーブル割り当て状況表示)
bridgestat -s [-I <interface>] (STP 状態表示)

[オプション]

オプションを指定しなかった場合は、-l を指定したものとみなされます。また、STP が有効なときは、-s を指定したものとみなされます。

-i

インタフェースごとの入出力パケット数を表示します。

-l

学習テーブルの情報を表示します。

-t

学習テーブルの割り当て状況を表示します。

-s

STP の状態を表示します。

[パラメタ]

-I <interface>

表示するインタフェースを指定します。

[説明]

ブリッジに関する状態、または統計情報を表示します。

[例]

以下に、表示例および表示内容を示します。

インタフェースごとの入出力パケット数を表示する場合 (-i 指定時)

```
# bridgestat -i
Name    Status  STP             In     Out
----    ------  ---             --     ---
(1)       (2)   (3)             (4)    (5)

lan0    valid   Listening        0       0
rmt0    valid   Listening        0       0
```

1) インタフェース名

2) ブリッジの状態
以下のいずれかが表示されます。

valid ブリッジは有効

invalid ブリッジは無効

3) STP の状態
   以下のいずれかが表示されます。

   not use　STP は無効

   Listening
   Listening 状態

   Learning　Learning 状態

   Forwarding
   Forwarding 状態

4) 入力パケット数

5) 出力パケット数

学習テーブルの情報を表示する場合 (-l 指定時)

```
# bridgestat -l
HashNo.  MAC address        Name    PortNo.  Status   Age
-------  -----------        ----    -------  ------   ---
  (1)        (2)             (3)      (4)     (5)     (6)

11       00:a0:c9:67:e1:4b  lan0    1        Used     297
```

1) 学習テーブルが登録されている Hash 番号

2) 学習テーブルに登録されている MAC アドレス

3) エントリされた端末が存在するインタフェース名

4) ポート番号

5) 学習テーブルの状態
   以下のいずれかが表示されます。

   Used　使用中

   unUsed　解放済み

6) 残り生存時間 (秒)

学習テーブルの割り当て状況を表示する場合 (-t 指定時)

```
# bridgestat -t
use        free       max alloc  learn      delete     expire
---        ----       ---------  -----      ------     ------
(1)        (2)           (3)      (4)        (5)        (6)

6          1021       6          6          0          0
```

1) 使用中の学習テーブル数

2) 未使用の学習テーブル数

3) 過去に割り当てられた学習テーブルの最大値

4) 学習テーブルにエントリした回数

5) 学習テーブルに空きがないために削除された学習テーブル数

6) 寿命によって削除された学習テーブル数

STP 情報を表示する場合 (-s 指定時)

```
# bridgestat -s
[lan0]
status             : Forwarding --- (1)
Root ID            : 8000-00:00:0e:58:00:6e --- (2)
Designated bridge  : 8000-00:00:0e:58:00:6e --- (3)
Path cost          : 00000000 --- (4)
Max age            : 20       --- (5)
Message age        : 0        --- (6)
Hello time         : 2        --- (7)
Forward delay      : 15       --- (8)

[rmt0]
status             : Forwarding --- (1)
Root ID            : 8000-00:00:0e:58:00:6e --- (2)
Designated bridge  : 8000-00:00:0e:58:00:6e --- (3)
Path cost          : 00000000 --- (4)
Max age            : 20       --- (5)
Message age        : 0        --- (6)
Hello time         : 2        --- (7)
Forward delay      : 15       --- (8)

[rmt2]
status             : not use  --- (1)
```

1) STP の状態
   以下のいずれかが表示されます。

   not use STP は無効

   Listening
   Listening 状態

   Learning Learning 状態

   Forwarding
   Forwarding 状態

2) ルートブリッジ ID
   ルートブリッジの ID が、「優先度-MAC アドレス」の形式で表示されます。

3) 代表ブリッジ ID
   代表ブリッジの ID が、「優先度-MAC アドレス」の形式で表示されます。

4) パスコスト値
   ルートブリッジまでのパスコスト値が表示されます。

5) 最大待ち合わせ時間 (秒)
   構成情報 BPDU の最大待ち合わせ時間 (秒) が表示されます。

6) 経過時間 (秒)
   ルートブリッジが送出した構成情報 BPDU が自装置に届くまでの経過時間 (秒) が表示されます。

7) 送出間隔 (秒)
   構成情報 BPDU の送出間隔 (秒) が表示されます。

8) 最大中継遅延時間 (秒)
   最大中継遅延時間 (秒) が表示されます。

15.4.4　natstat

[機能]

NAT 状態と統計情報の表示

[入力形式]

natstat
natstat -s
natstat -t [<interface>]

[オプション]

-s

NAT の統計情報を表示します。以下の情報が表示されます。

- プライベート→グローバル変換回数
- グローバル→プライベート変換回数
- プライベート→グローバルエラー発生回数
- グローバル→プライベートエラー発生回数
- フラグメントパケットの正常変換回数
- フラグメントパケットのエラー発生回数
- 現在使用中の NAT 変換テーブル個数
- NAT 変換テーブルのピークホールド個数 (NAT モジュールで確保した NAT 変換テーブル個数)
- メモリ枯渇回数
- 変換テーブルにないパケットの受信回数
- 異常に短いパケットの受信回数
- その他のエラー回数

-t

NAT 変換テーブルを一覧表示します。以下の情報が表示されます。

- インタフェース名
- 変換テーブル数
- 変換テーブル通番
- グローバル IP アドレス
- グローバルポート番号
- グローバル ICMP_ID
- プライベート IP アドレス
- プライベートポート番号
- プライベート ICMP_ID
- 相手側 IP アドレス
- 相手側ポート番号
- テーブル解放残時間 [*10 秒]

[パラメタ]

<interface>

インタフェース名を指定します。

[説明]

NAT 統計情報または変換テーブルを表示します。
オプション指定がない場合は、-s を指定したものとみなされます。

[例]

以下に、表示例および表示内容を示します。

統計情報

```
# natstat -s
*** NAT stat information ***
            to Global     to Private
translate         (1)          (2)
error             (3)          (4)

            fragment
translate         (5)
error             (6)

             current          peak
nat table         (7)           (8)

                           current
nat fragment table             (9)

error accounting
  lack of memory              (10)
  table not found             (11)
  too small packet            (12)
  other reason                (13)
```

1) プライベート→グローバル変換回数
2) グローバル→プライベート変換回数
3) プライベート→グローバルエラー発生回数
4) グローバル→プライベートエラー発生回数
5) フラグメントパケットの正常変換回数
6) フラグメントパケットのエラー発生回数
7) 現在使用中の NAT 変換テーブル個数
8) NAT 変換テーブルのピークホールド個数 (NAT モジュールで確保した NAT 変換テーブル個数)
9) 現在使用中の NAT 変換フラグメント変換テーブル個数
10) メモリ枯渇回数
11) 変換テーブルにないパケットの受信回数
12) 異常に短いパケットの受信回数
13) その他のエラー回数

変換テーブル表示

```
# natstat -t
*** NAT table information ***
I/F : (1)
[NAT table]   tblnum:(2)
index GlobalAddr/Port       PrivateAddr/Port      DestAddr/Port         remain
      GlobalAddr:Icmp_Id    PrivateAddr:Icmp_Id   DestAddr
[(3)] (4)/(5)               (7)/(8)               (10)/(11)             (12)
[(3)] (4):(6)               (7):(9)               (10)
```

1) インタフェース名

2) 変換テーブル数
3) 変換テーブル通番
4) グローバル IP アドレス
5) グローバルポート番号
6) グローバル ICMP_ID
7) プライベート IP アドレス
8) プライベート ICMP_ID
9) プライベートポート番号
10) 相手側 IP アドレス
11) 相手側ポート番号
12) テーブル解放残時間 [*10 秒]

統計情報

```
# natstat -s
*** NAT stat information ***
           to Global   to Private
translate         518          513
error               0            0

            fragment
translate           0
error               0

             current         peak
nat table           6           10

                           current
nat fragment table               0

error accounting
  lack of memory                 0
  table not found                0
  too small packet               0
  other reason                   0
```

変換テーブル表示

```
# natstat -t
*** NAT table information ***
I/F : unassigned
[NAT table]   tblnum:0

I/F : rmt0
[NAT table]   tblnum:12
index  GlobalAddr/Port       PrivateAddr/Port      DestAddr/Port         remain
[   0] 202.219.172.130/10009 192.168.1.3/1951      210.150.23.240/80          1
[   1] 202.219.172.130/10008 192.168.1.3/1950      210.150.23.240/80          1
[   2] 202.219.172.130/10007 192.168.1.3/1949      210.150.25.37/80          28
[   3] 202.219.172.130/10006 192.168.1.3/1948      210.150.23.240/80          1
[   4] 202.219.172.130/10005 192.168.1.3/1947      210.150.23.240/80          1
[   5] 202.219.172.130/10004 192.168.1.3/1946      210.150.25.37/80           1
[   6] 202.219.172.130/10003 192.168.1.3/1945      210.150.25.37/80           1
[   7] 202.219.172.130/10002 192.168.1.3/1944      210.150.25.37/80           1
[   8] 202.219.172.130/10001 192.168.1.3/1943      210.150.25.37/80          28
[   9] 202.219.172.130/0     192.168.1.3/0         0.0.0.0/0                  0
[  10] 202.219.172.130/53    192.168.1.50/53       202.248.2.209/53          28
[  11] 202.219.172.130/0     192.168.1.50/0        0.0.0.0/0                  0
```

15.4.5 ipsecstat

[機能]

システムの IPsec / IKE 情報の表示

[入力形式]

ipsecstat [<protocol>]

[オプション]

なし

[パラメタ]

<protocol>

isakmp ISAKMP SA 情報の表示

ipsec IPsec SA および SPD 情報の一括表示

[説明]

(1) オプションなし

```
# ipsecstat
[IPsec SA Information]
[1]     Remote Name(ISP-0), rmt0
        Side(Initiator), Gateway(192.168.2.1, 192.168.1.1), OUT
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=171237444(0x0a34e044)
        Created(Sep 29 17:59:03 2002), NewSA(23040secs, 3276Kbyte)
        Lifetime(28800secs), Current(332secs), Remain(28468secs)
        Lifebyte(4096Kbyte), Current(2528Kbytes), Remain(1568Kbyte)

[2]     Remote Name(ISP-0), rmt0
        Side(Initiator), Gateway(192.168.1.1, 192.168.2.1), IN
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=181913669(0x0ad7c845)
        Created(Sep 29 17:59:03 2002), NewSA(23040secs, 3276Kbyte)
        Lifetime(28800secs), Current(332secs), Remain(28468secs)
        Lifebyte(4096Kbyte), Current(2528Kbytes), Remain(1568Kbyte)

[IKE SA Information]
[1]     Destination(192.168.1.1.500), Source(192.168.2.1.500)
        Cookies(2ee33635dcc2a837:ece2a45bc12889ef)
        Side(Initiator), Status(ESTABLISHED), Exchangetype(AGGRESSIVE)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        Created(Sep 29 17:59:03 2002)
        Lifetime(86400secs), Current(10secs), Remain(86390secs)
```

(2) isakmp オプション指定

```
# ipsecstat isakmp
[1]     Destination(192.168.1.1.500), Source(192.168.2.1.500)
        Cookies(2ee33635dcc2a837:ece2a45bc12889ef)
        Side(Initiator), Status(ESTABLISHED), Exchangetype(AGGRESSIVE)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        Created(Sep 29 17:59:03 2002)
        Lifetime(86400secs), Current(10secs), Remain(86390secs)
```

(3) ipsec オプション指定

```
# ipsecstat ipsec
[1]     Remote Name(ISP-0), rmt0
        Side(Initiator), Gateway(192.168.2.1, 192.168.1.1), OUT
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=171237444(0x0a34e044)
        Created(Sep 29 17:59:03 2002), NewSA(23040secs, 3276Kbyte)
        Lifetime(28800secs), Current(332secs), Remain(28468secs)
        Lifebyte(4096Kbyte), Current(2528Kbytes), Remain(1568Kbyte)

[2]     Remote Name(ISP-0), rmt0
        Side(Initiator), Gateway(192.168.1.1, 192.168.2.1), IN
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=181913669(0x0ad7c845)
        Created(Sep 29 17:59:03 2002), NewSA(23040secs, 3276Kbyte)
        Lifetime(28800secs), Current(332secs), Remain(28468secs)
        Lifebyte(4096Kbyte), Current(2528Kbytes), Remain(1568Kbyte)
```

IPsec SA/SPD 情報

```
[1]     Remote Name(ISP-0), rmt0
 *1     *2                  *5
[1]     Destination(192.168.2.20/24), Source(192.168.1.10/24), rmt0
 *1     *3                      *4                      *5
        Side(Initiator), Gateway(192.168.2.1, 192.168.1.1), OUT
        *6              *7                              *8
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        *9             *10              *11             *12
        Status(mature), Spi=171237444(0x0a34e044)
        *13            *14
        Created(Sep 29 17:59:03 2002), NewSA(23040secs, 3276Kbyte)
        *15                           *16
        Lifetime(28800secs), Current(332secs), Remain(28468secs)
        *17                 *18               *19
        Lifebyte(4096Kbyte), Current(2528Kbytes), Remain(1568Kbyte)
        *20                 *21                 *22
```

***1 :** IPsec SA / SPD 表示番号

***2 :** IPsec 対象区間のネットワーク名 (Aggressive モードで IPsec 区間が any の場合)

***3 :** IPsec 対象宛先 IP アドレス (*2 の条件以外の場合)

***4 :** IPsec 対象送信元 IP アドレス (IPsec 区間の指定がある場合)

***5 :** IPsec 対象区間のインタフェース名 (Aggressive モード以外で特定インタフェースが指定されない場合は any と表示)

***6 :** ネゴシエーションサイド

Initiator: イニシエータ

Responder:
レスポンダ

Manual : 手動鍵設定 (*12 / *17 / *16 / *19 / *20 / *22 は、—で表示されます)

***7 :** IPsec 対象パケットをセキュア / アンセキュア化する送信元 IP アドレスおよび宛先 IP アドレス (IKE セッション)

***8 :** ポリシーの方向

OUT: 出力用ポリシー

IN : 入力用ポリシー

***9 :** 使用するセキュリティプロトコル

***10:** 暗号アルゴリズム

***11:** 認証アルゴリズム

***12:** PFS グループ

***13:** IPsec SA の状態

larval: IPsec SA 作成中状態 (ネゴシエーション中の状態)

mature: IPsec SA 作成完了状態 (ネゴシエーションが完了し、IPsec SA が作成された状態)

dying : SA の更新時間 (softtime) に到達した状態

※ IPsec 通信に使用されるのは、mature または dying の状態の IPsec SA となります。

***14:** SPI 値

***15:** IPsec SA 作成時間 (秒)

***16:** IPsec SA の更新を開始する時間 (秒) および有効パケット量 (キロバイト)

***17:** IPsec SA 有効時間 (秒)

***18:** IPsec SA 作成からの経過時間 (秒)

***19:** IPsec SA 削除までの残存時間 (秒)

***20:** IPsec SA 有効パケット量 (キロバイト)

***21:** IPsec SA 作成からの転送バイト数 (キロバイト)

出力時: 暗号化／認証後のパケット長の累計

入力時: 復号化／認証前のパケット長の累計

***22:** IPsec SA 削除までの残バイト数 (キロバイト)

ISAKMP SA 情報

```
[1]     Destination(192.168.1.1.500), Source(192.168.2.1.500)
*1      *2                            *3
        Cookies(2ee33635dcc2a837:ece2a45bc12889ef)
        *4
        Side(Initiator), Status(ESTABLISHED), Exchangetype(AGGRESSIVE)
        *5               *6                   *7
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        *8                *9                   *10
        Created(Sep 29 17:59:03 2002)
        *11
        Lifetime(86400secs), Current(10secs), Remain(86390secs)
        *12                  *13              *14
```

***1 :** ISAKMP SA 表示番号

***2 :** ISAKMP 宛先 IP アドレス

***3 :** ISAKMP 送信元 IP アドレス

***4 :** クッキー (Initiator:Responder)

***5 :** ネゴシエーションサイド

Initiator: イニシエータ

Responder:

レスポンダ

***6 :**　ISAKMP SA のネゴシエーション状態

MSG1RECEIVED
MSG1SENT
MSG2RECEIVED
MSG2SENT
MSG3RECEIVED
MSG3SENT
MSG4RECEIVED
ESTABLISHED
EXPIRED

※　ESTABLISHED は、Phase1 のネゴシエーションが完了した状態を意味します。
EXPIRED は、ISAKMP SA 情報の削除待ちを意味します。
その他は、Phase1 のネゴシエーション中の状態を意味します。

***7 :**　交換モード

BASE:　Base モード (未サポート)

MAIN:　Main モード

AUTH ONLY:
Authentication Only モード (未サポート)

AGGRESSIVE:
Aggressive モード

***8 :**　暗号アルゴリズム

***9 :**　認証アルゴリズム

***10:**　PFS グループ

***11:**　ISAKMP SA 作成時間

***12:**　ISAKMP SA 有効時間 (秒)

***13:**　ISAKMP SA 作成からの経過時間 (秒)

***14:**　ISAKMP SA 削除までの残存時間 (秒)

15.4.6 vrrpstat

[機能]

VRRP 機能における各種情報の表示

[入力形式]

vrrpstat [[-g] [<lan_number> [<vrid>]]]
vrrpstat -G <lan_number> <vrid>

[オプション]

-g

グループ簡易情報を表示

-G

グループ簡易情報を表示 (ヘッダなし)

[パラメタ]

<lan_number>

コマンド適用対象の LAN インタフェースを指定します。

- lan 定義番号
  lan 定義番号として、0 を指定します。

<vrid>

コマンド適用対象の VRRP グループを指定します。

- VRID
  VRRP グループの VRID を、1〜255 の 10 進数値で指定します。

[説明]

オプションなしの場合は、VRRP グループの詳細情報を表示します。
<lan_number>と<vrid>の両方を指定した場合は、指定 LAN インタフェースの指定 VRRP グループ詳細情報を表示します。
<lan_number>のみを指定した場合は、指定 LAN インタフェースに設定されたすべての VRRP グループ詳細情報を表示します。
<lan_number>と<vrid>の両方を指定しない場合は、全 VRRP グループの詳細情報を表示します。
-g オプションを指定することによって、VRRP グループ簡易情報を表示します。
-g オプションのみ指定した場合は、全 VRRP グループの簡易情報を表示します。
<lan_number>と<vrid>の両方を指定した場合は指定 LAN インタフェースの指定 VRRP グループ簡易情報を表示します。
<lan_number>のみ指定した場合は、指定した LAN インタフェースに設定されたすべての VRRP グループ簡易情報を表示します。
-G オプションを指定することによって、VRRP グループ簡易情報を表示します。
-G オプションを指定した場合、<lan_number>と<vrid>を指定しなくてはなりません。指定 LAN インタフェースの指定 VRRP グループ状態のみを表示します。

[例]

-g オプション

VRRP グループに関する簡易情報を表示します。
定義されている VRID の一覧とそのグループの状態を表示します。グループの状態として、
Master / Backup / Initialize があります。

- Master :
  マスタルータとして仮想ルータの IPv4 アドレス宛のパケットをフォワーディングしている状態。
- Backup :
  バックアップルータとしてマスタルータのダウンに備えている状態。
- Initialize :
  マスタルータまたはバックアップルータになることができない状態。

```
# vrrpstat -g
<LAN 0>
  VRID  Status
    10  Master

#
```

-G オプション

VRRP グループに関する情報を表示します。
指定した VRRP グループの状態を表示します。グループの状態として Master / Backup / Initialize があります。

```
# vrrpstat -G 0 10
    10  Master

#
```

オプションなし

オプションが指定されない場合は、VRRP グループについての詳細情報を表示します。

```
# vrrpstat
[LAN 0]
  State              : OK
  Authentication Type: Text
  Authentication Pass: "fujitu"
  Interface statistics information:
      0          Bad checksum packets
      0          VRRP Version illegal packets
      0          VRID illegal packets

  VRID 10
    Master(PRI 255 now 255/PREEMPT ON)
    Now Master : Me
    Virtual MAC Address : 00:00:5E:00:01:0A
    Virtual Router IP Address:
        10.124.2.126
        10.124.2.224
    VRRP advertisement interval 1
    Shutdown interface trigger:
        rmt11 reduce 100  OFF
    Shutdown route trigger:
        default            lan0  reduce 255  OFF
        10.232.79.200/32   rmt1  reduce 100  OFF
    Shutdown node trigger:
        10.232.79.193   rmt1  reduce 100  OFF
    Group statistics information:
        1          become master-router
        0          received VRRP advertisement packets
        0          VRRP advertisement interval configuration mismatched packets
        0          Authentication failed packets
        0          TTL illegal packets
        0          received priority 0 advertisement packets
        0          sent priority 0 advertisement packets
        0          VRRP type illegal packets
        0          Virtual router IP address configuration mismatched packets
        0          Authentication type illegal packets
        0          Authentication type mismatch packets
        0          Length illegal packets

  VRID 20
    Backup(PRI 100 now 50/PREEMPT OFF)
    Now Master : 10.124.2.100 Priority 255
    Virtual MAC Address : 00:00:5E:00:01:14
    Virtual Router IP Address:
        10.124.2.138
        10.124.2.139
    VRRP advertisement interval 1
    Shutdown interface trigger:
        rmt1  reduce 100  OFF
    Group statistics information:
        0          become master-router
        0          received VRRP advertisement packets
        0          VRRP advertisement interval configuration mismatched packets
        0          Authentication failed packets
        0          TTL illegal packets
        0          received priority 0 advertisement packets
        0          sent priority 0 advertisement packets
        0          VRRP type illegal packets
        0          Virtual router IP address configuration mismatched packets
        0          Authentication type illegal packets
        0          Authentication type mismatch packets
        0          Length illegal packets

#
```

2 情報を表示する LAN インタフェースの番号

3 LAN インタフェースの状態 : OK / NG

4 LAN インタフェースの VRRP パケット認証方法

5 LAN インタフェースの VRRP パケット認証パスワード

7 受信 VRRP パケットチェックサム異常数

8	受信 VRRP パケット VRRP バージョン異常数
9	受信 VRRP パケット VRID 異常数
11	VRID
12	VRRP グループ状態 (設定優先度、現在の優先度 / プリエンプトモード) VRRP グループ状態 : 現在の VRRP グループの状態 (Master / Backup / Initialize) 設定優先度 : 構成定義で設定された優先度 現在の優先度 : トリガイベントの減算値を含めた現在の優先度 プリエンプトモード : 構成定義で設定されたプリエンプトモード (ON / OFF)
13	現在のマスタルータの実 IPv4 アドレスと優先度 (自装置がマスタルータである場合は"Me" を表示)
14	仮想 MAC アドレス
15-17	仮想ルータの IPv4 アドレス
18	VRRP-AD の送信間隔
19-20	インタフェースダウントリガと適用状態
21-23	ルートダウントリガと適用状態
24-25	ノードダウントリガと適用状態
27	マスタルータになった回数
28	VRRP-AD 総受信数
29	受信 VRRP-AD 送信間隔異常数
30	受信 VRRP-AD 認証パスワード異常数
31	受信 VRRP-AD TTL 異常数
32	優先度 0 の VRRP-AD 総受信数
33	優先度 0 の VRRP-AD 総送信数
34	受信 VRRP パケットタイプ異常数
35	受信 VRRP-AD バックアップ IPv4 アドレス構成異常数
36	受信 VRRP-AD 認証タイプ異常数
37	受信 VRRP-AD 認証タイプ不一致数
38	受信 VRRP-AD ヘッダ長異常数

15.4.7 mhstat

[機能]

マルチホーミングの状態と統計情報の表示

[入力形式]

mhstat

[オプション]

なし

[パラメタ]

なし

[説明]

動的に作成されたマルチホーミングのセッション管理テーブルの情報、およびマルチホーミングに関する各種統計情報を表示します。
静的マルチホーミングとして設定した情報は、表示されません。

[例]

以下に表示例を示します。

```
# mhstat
WAN route
index  SrcAddr         DstAddr         type      remain(min)
-(1)-  --(2)--         --(3)--         -(4)-     --(5)------
[   0] 202.219.172.130 192.168.1.3     FTP       5
[   1] 202.219.172.130 192.168.1.3     DYNAMIC   14
[   2] 202.219.172.132 192.168.1.4     DYNAMIC   1
[   3] 202.219.172.135 192.168.1.9     DYNAMIC   8

multihoming forwarding (LAN) route
index  SrcAddr         DstAddr         type      remain(min)
-(6)-  --(7)--         --(8)--         -(9)-     --(10)-----
[   0] 202.219.172.131 192.168.1.7     DYNAMIC   3
[   1] 202.219.172.131 192.168.1.4     DYNAMIC   2
[   2] 202.219.172.132 192.168.1.3     DYNAMIC   6

multihoming information
  WAN route error                       4  --- (11)
  multihoming forwarding route error   15  --- (12)
  dynamic multihoming table full        1  --- (13)
```

WAN 側セッション (WAN route) に関する情報が表示されます。

1) テーブル番号
2) 送信元アドレス
3) 宛先アドレス
4) タイプ

   - DYNAMIC
     FTP 以外の動的マルチホーミング情報
   - FTP
     FTP の PORT コマンドによって作成されたマルチホーミング情報

5) セッションのタイムアウトまでの時間 (分)
転送セッション (multihoming forwarding (LAN) route) に関する情報が表示されます。
6) テーブル番号
7) 送信元アドレス
8) 宛先アドレス
9) タイプ
   - DYNAMIC
     FTP 以外の動的マルチホーミング情報
   - FTP
     FTP の PORT コマンドによって作成されたマルチホーミング情報
10) セッションのタイムアウトまでの時間 (分)
マルチホーミングの各種情報 (multihoming information) が表示されます。
11) WAN 側セッションの経路の障害発生件数
12) 転送セッションの経路の障害発生件数
13) 動的マルチホーミング情報テーブルの情報数が最大数に達した回数

15.5　ログ、トレースの表示

15.5.1　elog

[機能]

エラーログの表示

[入力形式]

elog

[オプション]

なし

[パラメタ]

なし

[説明]

ROM または I/O ドライバによるハード診断エラー、およびシステムダウンのエラーログ情報を表示します。

[注意]

"Logging time:"で表示する時刻は、構成定義情報にタイムゾーン (time zone <offset>) が指定されていない状態では GMT(グリニッジ標準時間) での表示となります。

[例]

以下に、表示例を示します。

```
# elog
[0] Error Log:
flag=80,mode=00,unit=80,regsp=00acba38
System down information:
down code [00000080:00001400]
Logging time:
Fri May  9 09:01:23 2008
Register:
SPR:    srr0 [0017d7e0] srr1 [0000d012] lr   [0017d7b0] dar  [00ffc000]
        dsisr[000010bd] sivec[3c000000] simsk[fffc0000]
GPR:    gpr00[0017d7b0] gpr01[00acbb08] gpr02[00000005] gpr03[00acbb1a]
        gpr04[0025fb40] gpr05[00000000] gpr06[00000000] gpr07[00000001]
        gpr08[00000000] gpr09[00acbb10] gpr10[00acbb18] gpr11[00acbae8]
        gpr12[0000000a] gpr13[00000000] gpr14[00000000] gpr15[00000000]
        gpr16[00000000] gpr17[00000000] gpr18[00000000] gpr19[00000000]
        gpr20[00000000] gpr21[00260000] gpr22[00260000] gpr23[00260000]
        gpr24[00308110] gpr25[00000000] gpr26[00000001] gpr27[00000008]
        gpr28[00ffc000] gpr29[00ffc000] gpr30[00000000] gpr31[00acbb1a]


#
```

15.5.2　dsplog

[機能]

syslog メッセージの表示

[入力形式]

dsplog

[オプション]

なし

[パラメタ]

なし

[説明]

syslog メッセージの履歴を表示します。最新のメッセージからさかのぼって、128 件分表示できます。

[例]

以下に、表示例を示します。

```
# dsplog
Sep 19 18:03:14 init: system startup now.
Sep 19 18:03:14 protocol: line synchronization is established
```

15.5.3 llog

[機能]

回線ログの表示

[入力形式]

llog

[オプション]

なし

[パラメタ]

なし

[説明]

ISDN 回線の発着呼エラー、非同期エラー、認証エラー、または発呼契機パケットのログ情報を表示します。

[例]

以下に表示例を示します。

```
# llog
[01] B1ch : WAN  callout failed (other reason)          2000.01.02  09:15:16
        status : 00000030 state : 00 reason : 8483(#3)

[02] B1ch : CALL to "simple"    by ProxyDNS             2000.01.02  09:15:29

[03] B1ch : WAN  callout failed (other reason)          2000.01.02  09:15:31
        status : 00000030 state : 00 reason : 8483(#3)
#
```

15.5.4　ppptrace

[機能]

PPP フレームトレースの表示

[入力形式]

ppptrace

[オプション]

なし

[パラメタ]

なし

[説明]

PPP フレームトレース情報を表示します。

[注意]

PPP フレームトレース情報は、本装置を再起動するとクリアされます。

[例]

以下に、表示例および表示内容を示します。

```
# ppptrace
[01] B1ch : PPP session start                          00.01.02 09:19:54.225
---- ----   -----------------                          --------------------
(1)  (2)    (3)                                        (4)

[02] B1ch : Send LCP     Configure-Request id=0x00 len=18 00.01.02 09:19:54.226
---- ----   ---- ---     ----------------- ------- ------ --------------------
(1)  (2)    (5)  (6)     (7)               (8)     (9)    (4)
        data=c021 0100 0012 0104 05f4 0506 f015 8370
             0702 0802
        ------------------------------------------
        (10)

[03] B1ch : Send LCP     Configure-Request id=0x00 len=18 00.01.02 09:19:57.227
        data=c021 0100 0012 0104 05f4 0506 f015 8370
             0702 0802

[04] B1ch : Recv LCP     Configure-Request id=0x01 len=22 00.01.02 09:19:57.262
        data=c021 0101 0016 0104 05f4 0305 c223 0513
             0903 00c0 7b60 e186

[05] B1ch : Send LCP     Configure-Reject  id=0x01 len=13 00.01.02 09:19:57.264
        data=c021 0401 000d 1309 0300 c07b 60e1 86
```

(続く)

(続き)

```
[06] B1ch : Recv LCP     Configure-Reject  id=0x00 len=8  00.01.02 09:19:57.265
       data=c021 0400 0008 0702 0802

[07] B1ch : Send LCP     Configure-Request id=0x01 len=14 00.01.02 09:19:57.267
       data=c021 0101 000e 0104 05f4 0506 f015 8370

[08] B1ch : Recv LCP     Configure-Request id=0x02 len=13 00.01.02 09:19:57.280
       data=c021 0102 000d 0104 05f4 0305 c223 05

[09] B1ch : Send LCP     Configure-Ack     id=0x02 len=13 00.01.02 09:19:57.281
       data=c021 0202 000d 0104 05f4 0305 c223 05

[10] B1ch : Recv LCP     Configure-Ack     id=0x01 len=14 00.01.02 09:19:57.285
       data=c021 0201 000e 0104 05f4 0506 f015 8370

[11] B1ch : Recv CHAP    Challenge         id=0x01 len=26 00.01.02 09:19:57.301
       data=c223 0101 001a 10b2 8392 ffbe ae93 63a6
            6cb1 3b40 20e1 8d63 7331 6431

[12] B1ch : Send CHAP    Response          id=0x01 len=29 00.01.02 09:19:57.303
       data=c223 0201 001d 10ca 8988 13ed 8f52 d981
            e473 dac0 05ec 2a66 7767 6130 3034 34

[13] B1ch : Recv CHAP    Success           id=0x01 len=5  00.01.02 09:19:57.414
       data=c223 0301 0005 00

[14] B1ch : Send IPCP    Configure-Request id=0x00 len=22 00.01.02 09:19:57.419
       data=8021 0100 0016 0206 002d 0f00 0306 0000
            0000 8106 0000 0000

[15] B1ch : Recv CCP     Configure-Request id=0x01 len=10 00.01.02 09:19:57.420
       data=80fd 0101 000a 1106 0001 0103

[16] B1ch : Send LCP     Protocol-Reject   id=0x03 len=16 00.01.02 09:19:57.421
       data=c021 0803 0010 80fd 0101 000a 1106 0001
            0103

[17] B1ch : Recv IPCP    Configure-Request id=0x01 len=10 00.01.02 09:19:57.422
       data=8021 0101 000a 0306 cadb 883a

[18] B1ch : Send IPCP    Configure-Nak     id=0x01 len=10 00.01.02 09:19:57.423
       data=8021 0301 000a 0206 002d 0f00

[19] B1ch : Recv IPCP    Configure-Reject  id=0x00 len=10 00.01.02 09:19:57.436
       data=8021 0400 000a 0206 002d 0f00

[20] B1ch : Send IPCP    Configure-Request id=0x01 len=16 00.01.02 09:19:57.438
       data=8021 0101 0010 0306 0000 0000 8106 0000
            0000

[21] B1ch : Recv IPCP    Configure-Request id=0x01 len=10 00.01.02 09:19:57.445
       data=8021 0101 000a 0306 cadb 883a

[22] B1ch : Send IPCP    Configure-Ack     id=0x01 len=10 00.01.02 09:19:57.446
       data=8021 0201 000a 0306 cadb 883a

[23] B1ch : Recv IPCP    Configure-Nak     id=0x01 len=16 00.01.02 09:19:57.455
       data=8021 0301 0010 0306 cadb 8c53 8106 caf8
            02e2

[24] B1ch : Send IPCP    Configure-Request id=0x02 len=16 00.01.02 09:19:57.456
       data=8021 0102 0010 0306 cadb 8c53 8106 caf8
            02e2

[25] B1ch : Recv IPCP    Configure-Ack     id=0x02 len=16 00.01.02 09:19:57.473
       data=8021 0202 0010 0306 cadb 8c53 8106 caf8
            02e2

[26] B1ch : Send LCP     Terminate-Request id=0x03 len=4  00.01.02 09:21:16.085
       data=c021 0503 0004

[27] B1ch : Recv LCP     Terminate-Ack     id=0x03 len=4  00.01.02 09:21:16.099
       data=c021 0603 0004
```

1) ログ番号

ログ番号が、01～99 の 10 進数値で表示されます。

2) 回線識別子

通信に利用した回線が以下の形式で表示されます。

専用線の場合 : B1 が表示されます。

ISDN の場合 : チャネル名が表示されます。

3) ネゴシエーション開始

ネゴシエーション開始時に表示されます。

4) 採取時間

情報を採取した時間が表示されます。

5) 送受信

以下のいずれかが表示されます。

- Send
- Recv

6) プロトコル種別

PPP のプロトコル種別として、以下のプロトコルが表示されます。

プロトコル種別の前に「MP:」が付加されている場合、そのパケットが MP によってカプセル化されていることを示します。

```
Oxc021  LCP     : Link Control Protocol
Oxc023  PAP     : Password Authentication Protocol
Oxc223  CHAP    : Challenge-Handshake Authentication Protocol
Ox8021  IPCP    : Internet Protocol Control Protocol
Ox8031  BCP     : Bridge Control Protocol
Ox8057  IPV6CP  : IPv6 Control Protocol
Ox80fd  CCP     : Compression Control Protocol
Ox80fb  ICCP    : Individual Compression Control Protocol
Oxc02d  BAP     : Bandwidth Allocation Protocol
Oxc02b  BACP    : Bandwidth Allocation Control Protocol
Oxc029  CBCP    : Callback Control Protocol
```

7) コード種別

各プロトコルでのコードの内容が以下の文字列で表示されます。

- プロトコル種別が LCP、CCP、ICCP、IPCP、IPV6CP、BCP の場合

```
Ox01    Configure-Request
Ox02    Configure-Ack
Ox03    Configure-Nak
Ox04    Configure-Reject
Ox05    Terminate-Request
Ox06    Terminate-Ack
Ox07    Code-Reject
```

- プロトコル種別が LCP の場合

```
Ox08    Protocol-Reject
Ox09    Echo-Request
Ox0a    Echo-Reply
Ox0b    Discard-Request
```

- プロトコル種別が CCP、ICCP の場合

```
Ox0e    Reset-Request
Ox0f    Reset-Act
```

- プロトコル種別が PAP の場合

```
Ox01    Authenticate-Request
Ox02    Authenticate-Ack
Ox03    Authenticate-Nak
```

- プロトコル種別が CHAP の場合

```
Ox01    Challenge
Ox02    Response
Ox03    Success
Ox04    Failure
```

- プロトコル種別が BAP の場合

```
Ox01    Call-Request
Ox02    Call-Response
Ox03    Callback-Request
Ox04    Callback-Response
Ox05    Link-Drop-Request
Ox06    Link-Drop-Response
Ox07    Call-Status-Ind
Ox08    Call-Status-Rsp
```

- プロトコル種別が CBCP の場合

```
Ox01    Callback-Request
Ox02    Callback-Response
Ox03    Callback-Ack
```

8) ID フィールド値

PPP フレーム中の ID フィールドの値が、2 桁の 16 進数で表示されます。

9) パケット長

送受信したパケット長が、10 進数で表示されます。

10) data=

送受信したパケットの内容が、16 進数値で表示されます。最大 108 バイト分までが表示され、それよりあとは表示されません。

15.6　装置情報の表示

15.6.1　uptime

[機能]

システム起動時からの経過時間の表示

[入力形式]

uptime

[オプション]

なし

[パラメタ]

なし

[説明]

システム起動時からの経過時間を表示します。

[例]

以下に、表示例を示します。

```
# uptime
0000.01:20:22
#
```

15.6.2 idinfo

[機能]

ファームウェアのバージョン情報の表示

[入力形式]

idinfo

[オプション]

なし

[パラメタ]

なし

[説明]

ファームウェアの製品情報を表示します。
製品名、MAC アドレス、ROM 版数、ファーム版数が、順番に表示されます。

[例]

以下に、表示例および表示内容を示します。

```
# idinfo
Si-R130B --- (1)
00000ef10058 --- (2)
ROM:1.1 --- (3)
FIRM:V04.07 --- (4)
```

1) 製品名
   半角 20 文字以内で表示されます。
2) MAC アドレス
   12 桁の 16 進数値で表示されます。
3) ROM 版数
   xx.yy の形式で表示されます。xx、yy は 10 進数値で表示されます。
4) ファーム版数
   Vxx.yy の形式で表示されます。xx、yy は 2 桁の 10 進数値で表示されます。

15.7　その他の表示

15.7.1　help

[機能]

制御コマンド、表示コマンド の HELP 表示

[入力形式]

help [<command>]

[オプション]

なし

[パラメタ]

<command>

- コマンド 名

  制御コマンド 名、または表示コマンド 名を指定します。

  省略した場合は、使用可能なコマンド 一覧が表示されます。

[説明]

制御コマンド、表示コマンド のヘルプを表示します。

[例]

以下に、使用可能なコマンド 一覧を表示する場合の表示例を示します。

```
# help
*** control ***
 /logon         /exit          /reset         /save          /enable
 /connect       /disconnect    /addlink       /dellink       /timerctl
 /update        /ping          /date          /rdate         /rpon
 /rcmd          /rcmdctl       /dnconv        /emailcheck    /ping6
 /vrrpctl

*** display ***
 /uptime        /show          /netstat       /dhcpstat      /natstat
 /lineis        /isdnstat      /frstat        /elog          /llog
 /ppptrace      /dsplog        /stlan         /stins         /help
 /history       /bridgestat    /ipsecstat     /mhstat        /routestat
 /vrrpstat      /idinfo
```

第 16 章　シェル関連コマンド

16.1　env

[機能]

環境変数の表示 / 設定 / 削除

[入力形式]

env (表示)
env <name>=<value> (設定)
env -u <name> (削除)

[オプション]

-u
環境変数を削除する場合に指定します。

[パラメタ]

<name>
環境変数名を指定します。

<value>
環境変数値を指定します。

[説明]

環境変数を表示、設定、または削除します。
環境変数名と環境変数値の説明を以下に示します。

- PROMPT
  プロンプト文字列を指定します。
  文字列に空白が含まれる場合は、ダブルクォーテーション (") で囲みます。また、プロンプト文字列中にバックスラッシュで始まる特殊文字を含めると、以下のように展開した文字列に置き換わります。

特殊文字	展開文字列
\!	履歴番号
\p	標準プロンプト
\u	環境変数USERの値（ログオン前は無効)
\U	環境変数USERの値（ログオン前も有効)
\\	バックスラッシュ(\)1個

以下に、標準プロンプトを示します。

状　態	標準プロンプト
シリアルコンソール ログオン前 シリアルコンソール ログオン後 telnet ログオン後	>　 #　 #

ログオン前は履歴機能が無効なため、"\!"とそれに続く空白 1 つが無視されます。

環境変数 USER がない場合は、"\u"および"\U"とそれに続く空白 1 つが無視されます。

以下に、設定例を示します。

```
env PROMPT="\! \u \p"
```

- COLUMNS

  画面桁数を 10 進数値で指定します。1 以上を指定した場合に、設定が有効になります。

  実際の画面の桁数と違う値を指定すると、コマンド 入力時に表示やカーソル位置が乱れます。

  また、telnet ログオン時に画面サイズを変更した場合、自動的にシェル内部の桁数が変更され、本環境変数値は無効となります。ただし、画面サイズ変更後に本環境変数を設定すると、本環境変数値が有効となります。

- LINES

  画面行数を 10 進数値で指定します。1 以上を指定した場合に、設定が有効となります。

  画面行数を 13 行以下にすると、コマンド 入力時に表示やカーソル位置が乱れます。

  また、telnet でログオンしていて画面サイズを変更した場合、自動的にシェル内部の桁数が変更され、本環境変数値が無効となります。ただし、画面サイズ変更後に本環境変数を設定すると、本環境変数値が有効となります。

- KANJI

  漢字コード を指定します。コマンド 引数補完時の引数説明が指定した漢字コード で表示されます。

  環境変数値と漢字コード の対応を以下に示します。

環境変数値	漢字コード
SJIS EUC その他/なし	ShiftJIS EUC EUC

- USER

  ユーザ名を文字列で指定します。環境変数 PROMPT の"\u"や"\U"で使用されます。

- NOBELL

  シェルは、以下の場合にベルを鳴らします。

  - 最大文字数 (1022 文字) を超えて入力しようとした場合
  - 最大文字数 (1022 文字) を超える貼り付けを行った場合
  - 補完候補がない場合

  以下の値によってベルの動作を指定できます。

環境変数値	動　作
yes on その他/なし	鳴らさない 鳴らさない 鳴らす

- HISTSIZE

  履歴行数を 0～100 の 10 進数値で指定します。100 以上を指定しても、100 を指定したものとみなされます。0 を指定すると、履歴を残しません。

  行数を変更した場合、履歴番号や履歴内容は引き継がれますが、0 から増やした場合には履歴番号が 1 からになります。

  削除したり無効な値を指定すると、前の履歴行数のままとなります。

- SAVEENV

  環境変数は、“14.1.3 save” で構成定義情報と共に保存できます。環境変数 SAVEENV では、save コマンドで環境変数も保存するかどうかを指定します。

環境変数値	動　作
no off その他/なし	保存しない 保存しない 保存する

[注意]

環境変数を保存する場合、上記以外の環境変数はできるだけ設定しないでください。
PROMPT に空となるような文字列を指定すると、プロンプトが表示されず、入力できない状態のように見えますが、入力してコマンド実行することができます。

[未設定時]

以下に示すように環境変数が設定されているものとみなされます。

```
env PROMPT="\u\p"
env COLUMNS=80
env LINES=24
env KANJI=EUC
env -u USER
env NOBELL=no
env HISTSIZE=24
env SAVEENV=yes
```

16.2　history

[機能]

コマンド履歴の表示/消去

[入力形式]

history (表示)
history -c (消去)

[オプション]

-c

- 履歴削除
  履歴を消去する場合に指定します。

[パラメタ]

なし

[説明]

コマンド履歴を表示または削除します。
履歴を表示すると、履歴番号と履歴内容が一覧表示されます。履歴を編集中で実行していない行には、履歴番号の後ろに"*"が表示されます。"*"が表示されている場合は、以下のいずれかの方法で"*"を消すことができます。

- Ctrl+P キーまたは↑キーでその行を表示し、改行キーを押してコマンドを実行する。
- Ctrl+P キーまたは↑キーでその行を表示し、Ctrl+C を押して入力内容を破棄する。
- Ctrl+P キーまたは↑キーでその行を表示し、Ctrl+U を押して空行にしてほかの履歴に移動する。

履歴を消去すると、履歴番号は 1 からふり直されます。
履歴行数は、環境変数 HISTSIZE で変更できます。環境変数については、env を参照してください。

[注意]

履歴番号が 32767 を超えると、適当な小さい履歴番号にふり直されます。